National Defense Research Institute

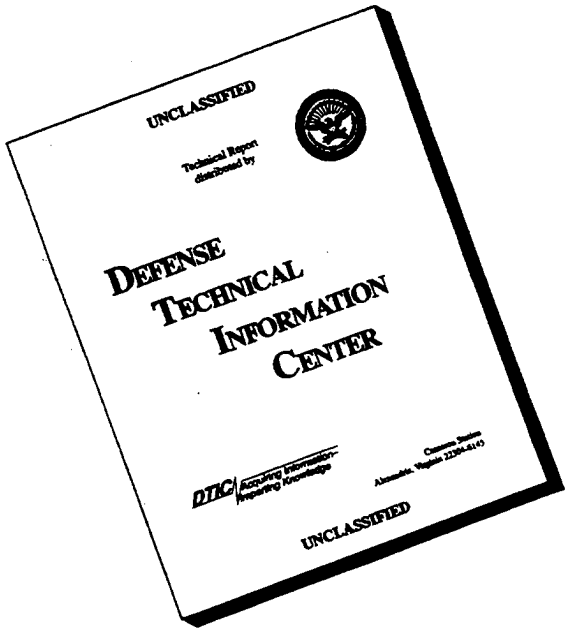
# THE ADVENT OF NETWAR



JOHN ARQUILLA

DAVID RONFELDT

# DISCLAIMER NOTICE




**THIS DOCUMENT IS BEST QUALITY AVAILABLE. THE COPY FURNISHED TO DTIC CONTAINED A SIGNIFICANT NUMBER OF PAGES WHICH DO NOT REPRODUCE LEGIBLY.**

The research described in this report was sponsored by the Office of the Secretary of Defense (OSD), under RAND's National Defense Research Institute, a federally funded research and development center supported by the OSD, the Joint Staff, and the defense agencies, Contract No. DASW01-95-C-0059/T001.

ISBN: 0-8330-2414-0



Published 1996 by RAND
1700 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact Distribution Services: Telephone: (310) 451-7002; Fax: (310) 451-6915; Internet: order@rand.org

National Defense Research Institute

# THE ADVENT OF NETWAR

JOHN ARQUILLA

DAVID RONFELDT



Prepared for the
Office of the Secretary of Defense

RAND

# PREFACE

This documented briefing was prepared for a project on new modes of information-age conflict titled "Advent of Netwar." That project is sponsored by the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence), OASD (C3I), and is being conducted within the Acquisition and Technology Policy Center of RAND's National Defense Research Institute (NDRI). NDRI is a federally funded research and development center sponsored by the office of the Secretary of Defense, the Joint Staff, and the defense agencies.

This document provides an overview of the "netwar" concept, which we have been developing for the purpose of better understanding the nature of conflict and crime in the information age. The document is based on several briefings that we have presented since May 1995 using charts like those included here.

A briefing is supposed to tell a story at a pace and in a way that attracts the listeners' attention, the better to inform them. Readers unfamiliar with the briefing style should be apprised that while the text is meant to expand on the points of the chart, not all points are always addressed in the text, and the text may not echo precisely the wording on a chart. That can be particularly true for a briefing with as many charts as this one.

Primarily of interest to U.S. government officials and policy analysts, this briefing should also interest those concerned with the changing nature of conflict and crime in the information age.

Comments are invited.

John Arquilla
Associate Professor
Dept. of National Security Affairs
U.S. Naval Postgraduate School
Monterey, CA 93943

(408) 656-3450
jarquilla@mntry.nps.navy.mil

David Ronfeldt
Senior Social Scientist
International Policy Group
RAND
Santa Monica, CA 90407-2138

(310) 393-0411
ronfeldt@rand.org

# CONTENTS

## SUMMARY

This briefing elucidates a concept—"netwar"—that we mentioned in an earlier article on "cyberwar." Whereas the latter term refers primarily to information-based military operations designed to disrupt an adversary, netwar relates to lower-intensity conflict at the societal end of the spectrum. In our view, netwar is likely to be the more prevalent and challenging form of conflict in the emerging information age and merits careful and sustained study.

In terms of conduct, netwar refers to conflicts in which a combatant is organized along networked lines or employs networks for operational control and other communications. The organizational forms that netwar actors adopt may resemble "stars" that have some centralized elements, or "chains" that are linear, but the major design will tend to be "all-channel" networks in which each principal node of an organization can communicate and interact with every other node. Further, netwar actors may develop hybrid structures that incorporate elements of some or all of the above designs in varied ways. Strong netwar actors will have not only organizational, but also doctrinal, technological, and social layers that emphasize network designs. Netwar actors may make heavy use of cyberspace, but that is not their defining characteristic—they subsist and operate in areas beyond it.

Because of changes in the context for possible conflict, netwar will no doubt prove most attractive, for the near-term future, to nonstate actors. It is likely to become a policy tool of choice for ethnonationalists, terrorists, and transnational criminal and revolutionary organizations. However, nation-states may increasingly find netwar a useful option, especially when the need to pursue limited aims with limited means arises. Additionally, the rise of a global civil society heralds the possibility that nongovernmental organizations associated with militant social activism will become netwar combatants, deliberately or sometimes inadvertently. Overall, the context of netwar may come to be defined by conflicts between state and nonstate actors, nonstate actors that use states as arenas, or states that use nonstate actors as their proxies.

The emergence of netwar implies a need to rethink strategy and doctrine, since traditional notions of war as a sequential process based on massing, maneuvering, and fighting will likely prove inadequate to cope with a nonlinear landscape of conflict in which societal and military elements are closely intermingled. In our view, traditional warfare fits the Western paradigm symbolized by chess, where territory is very

important, units are functionally specialized, and operations proceed sequentially until checkmate. Netwar, however, requires a new analytic paradigm, which, we argue, is provided by the Oriental game of Go, where there are no "fronts," offense and defense are often blurred, and fortifications and massing simply provide targets for implosive attacks. Victory is achieved not by checkmate, as there is no king to decapitate, but by gaining control of a greater amount of the "battlespace."

The equilibrium between offense and defense is another issue of concern. Historically, developments that change the context and/or conduct of war have generally introduced periods of offense- or defense-dominance. On the one hand, the science of fortification long gave the defensive great advantages. On the other hand, mechanization gave the advantage to the offensive. In each case, though, a reaction process occurred, which restored the equilibrium between offense and defense. With regard to netwar, we see an initial period of offense-dominance emerging. This requires the United States to focus on defensive netwar. Briefly, we find that the best chances for successful defense will arise when the defenders move toward more networked structures, emulating the organization, but not necessarily the tactics, of the attackers.

In terms of implications for policy, we argue that forming networks to fight networks and decentralizing operational decisionmaking authority will likely improve the ability of the United States to combat transnational crime and terrorism and to counter the proliferation efforts of rogue states and their nonstate support networks. Further, we urge the establishment of an "information war room" whose purpose would be to provide timely assessments of the netwar capabilities of plausible adversaries, including the preparation of detailed "information orders of battle."

Our concerns about the rapid emergence and likely profusion of netwars in the coming years lead us to call for the creation of a center devoted specifically to developing the means for countering this emergent form of conflict. The institute would serve both as a generator of and clearinghouse for ideas. The scope of activities would include the issue areas of strategy, doctrine, organization, and technology. In addition, an institute for the study of information should also emerge. It would address issues of society and security in the information age that go well beyond the pressing concerns of preparing to wage netwar. Indeed, this institute would help establish a new academic discipline, one that would address key political, economic, social, and military issue areas.

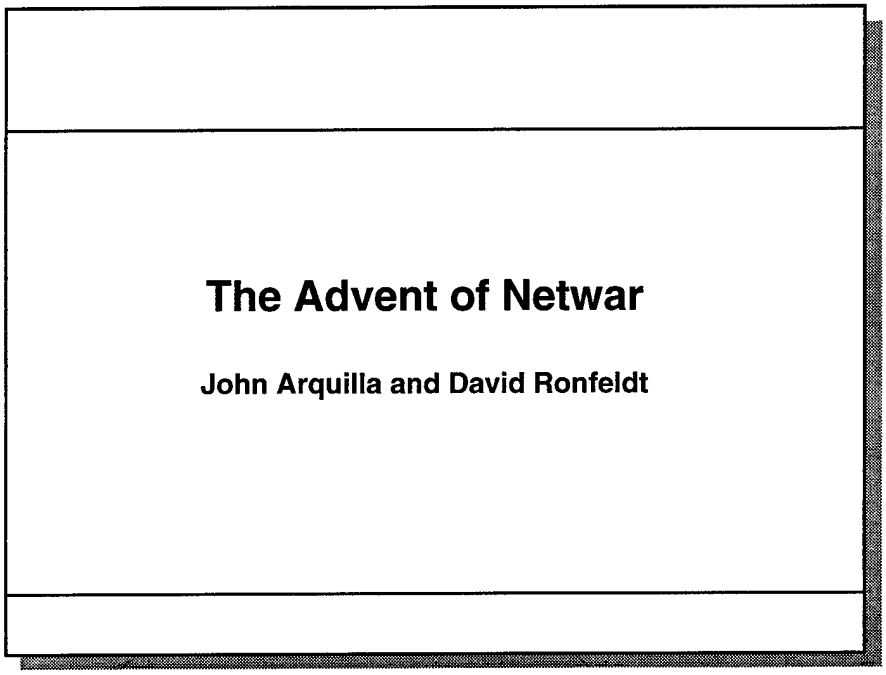
The report that follows addresses and outlines, we believe, the issues that ought to be studied in these two centers, and demonstrates the deductive and comparative methodologies that might be employed.

# ACKNOWLEDGMENTS

The authors thank RAND colleagues who work in the Acquisition and Technology Policy Center—notably, Bob Anderson, Carl Builder, Jim Gillogly, Gene Gritton, Dick Hundley, and Roger Molander—for their thoughtful comments and suggestions about conflict in the information age. Bob Nurick provided an incisive review that, among other things, helped clarify the presentation of the analytic framework and other ideas. Research assistant Ted Karasik and RAND Graduate School student Natalie Feldgun provided information about clan-based ethnic conflicts and transnational criminal organizations. Summer intern Armando Martínez was helpful, in the context of another project, with research on Mexico and the Zapatista movement. Eric Ellen, of the International Maritime Bureau, and LT Christopher Cobb (USN) shared their knowledge of East Asian pirates, and Gordon McCormick, of the Naval Postgraduate School, made available the comprehensive Violence at Sea Database. Barry Horton, principal deputy, and CAPT Richard O'Neill (USN), of the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (OASD/C3I) have provided both material support for our research and useful critiques of drafts of this study. The authors thank Christina Pitcher and Betty Amo for their editorial assistance.

Chapter One

# INTRODUCTION



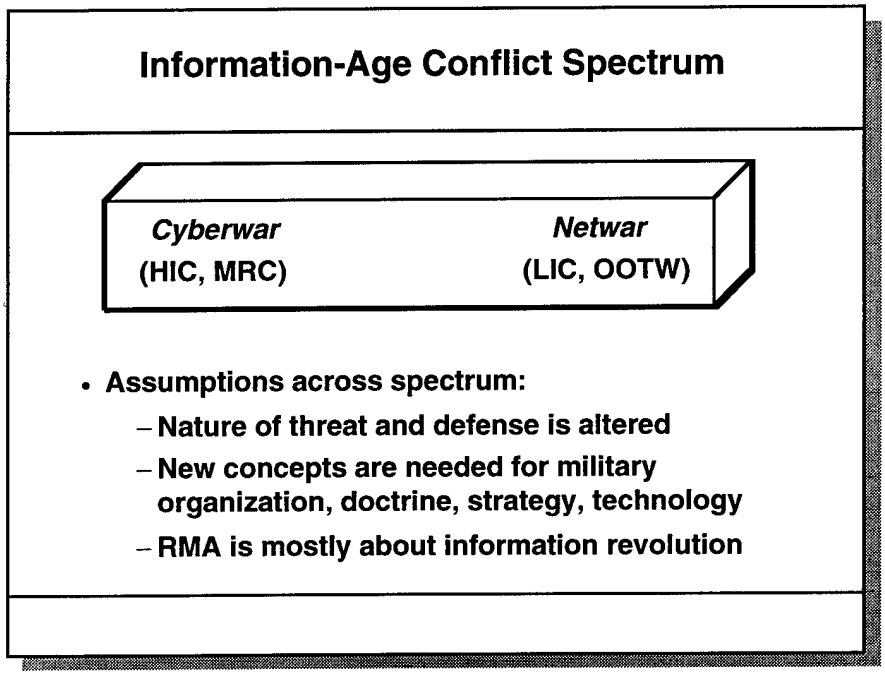

This documented briefing elucidates a concept—"netwar"—that we mentioned in an earlier paper on "cyberwar" (Arquilla and Ronfeldt, 1993).

At the time, we had begun to wonder about the implications of the information revolution for war and lesser modes of conflict. Our notion was that the information revolution would cause radical shifts in how societies come into conflict, and how their security forces should prepare and respond. When we coined the term "cyberwar" to discuss military implications for warfare, we realized that we needed a separate term to discuss conflicts short of war involving actors who may or may not be military. That term became "netwar."

Its distinguishing element is that at least one of the protagonists, usually a nonstate actor, organizes as a network rather than a hierarchy. Network designs have been used throughout history with mixed results. Today's information revolution, however, is making the network a much more effective form of organization, one that

may have overarching effects on society and security. For example, terrorist and criminal organizations are increasingly taking advantage of new information technologies to realize the full potential of highly decentralized, networked designs.

Netwar is blurring the line between peace and war, offense and defense, and combatant and noncombatant. As a result, the United States will face a new generation of nettlesome challenges that, in our view, will require new doctrines and strategies to combat them.




In our view, the information-age conflict spectrum looks like this: What we term "cyberwar" will be an ever-more-important entry at the military end, where the language is normally about high-intensity conflict (HIC) and middle-range conflict (MRC). "Netwar" will figure increasingly at the societal end, where the language is normally about low-intensity conflict (LIC) and operations other than war (OOTW—a broader concept than LIC that includes peacekeeping and humanitarian relief operations). Whereas cyberwar will usually see formal military forces pitted against each other, netwar is more likely to involve nonstate, paramilitary, and other irregular forces. Both concepts are consistent with the views of analysts like Van Creveld (1991) who believe that a transformation of war is under way, leading to increased "irregularization."

The terms above reflect two assumptions (or propositions) about the information revolution. One is that conflicts will increasingly depend on, and revolve around, information and communications—"cyber"—matters, broadly defined. Indeed, both

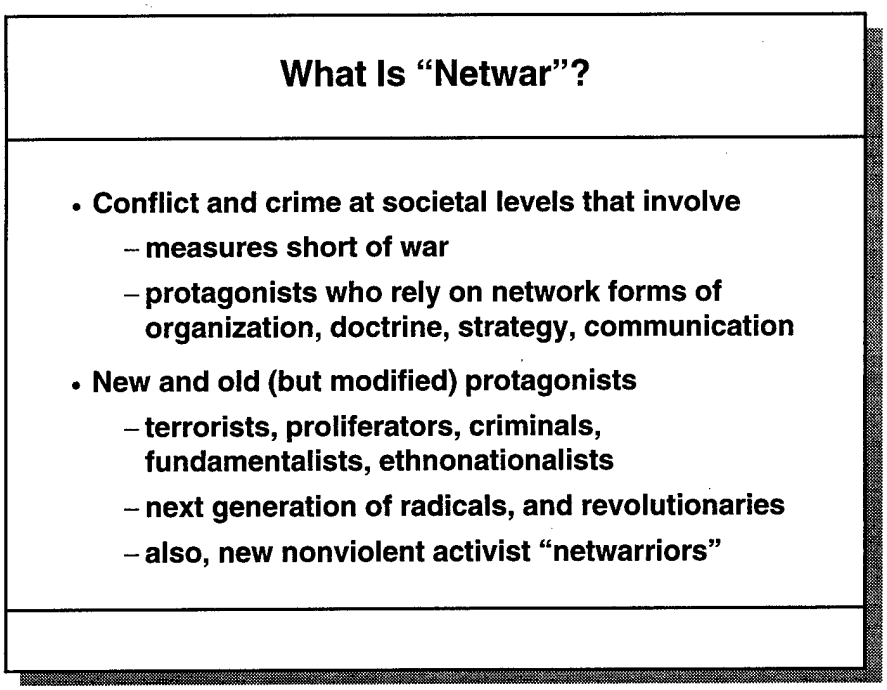
cyberwar and netwar are modes of conflict that are largely about "knowledge"—about who knows what, when, where, and why, and about how secure a society, military, or other actor is regarding its knowledge of itself and its adversaries.

The other assumption is that the information revolution favors and strengthens network forms of organization, while making life difficult for hierarchical forms. This implies that conflicts will increasingly be fought by "networks" more than by "hierarchies." Thus, whoever masters the network form should gain major advantages in the new era.

Both assumptions permeate this analysis and are discussed further as it proceeds. A point to emphasize here is that these assumptions affect the entire conflict spectrum. They mean that major alterations are looming in the nature of our adversaries, in the threats they pose, and for the defense measures the United States should consider. Information-age threats are likely to be more diffuse, nonlinear, and multidimensional than industrial-age threats. Cyberwars and netwars may even be mounted at the same time, in mixes that pose uncomfortable societal dilemmas. All this will place the U.S. military and society under increasing pressure to develop new concepts for organization, doctrine, strategy, tactics, and technology.

At present, the U.S. military is the world's leader with regard to thinking, planning, and preparing for cyberwar. The United States is the only country with an array of advanced technologies (e.g., for command, control, communications, and intelligence (C3I), surveillance, stealth, etc.) to make cyberwar an attractive and feasible option. But potential U.S. adversaries have the lead with regard to netwar. Here, the U.S. emphasis must be on defensive measures. This continues a long trend in which the United States has been prepared for waging major wars, while our adversaries may instead wage guerrilla warfare, terrorism, and other irregular modes of conflict. This may be partly the result of displacement—some adversaries, seeing that they should avoid or could not win at regular warfare, have opted for irregular modes, which the U.S. military may then try to treat as "lesser-included cases." Such displacement may occur again with netwar. But, hopefully, netwar will not be perceived as a "lesser-included case" of information-age conflict, for it is not.

Instead of using terms like cyberwar or netwar, many analysts have been treating such points under the rubric of the "revolution in military affairs" (RMA). Yet, this very general concept is still mainly about the information revolution and its effects and implications. It led early exponents to view technology innovation as the most important dimension of the RMA. But other, recent exponents have come to accept that the RMA is equally if not mainly about organizational and doctrinal innovation—a view we have emphasized since beginning our efforts to conceptualize cyberwar and netwar. Even so, discussions about the RMA tend to focus on HICs and MRCs that revolve around regular, albeit much-modified military forces. Exponents of the RMA have had less to say about the netwar end of the spectrum (see Arquilla and Ronfeldt, 1995).




The term "netwar" denotes an emerging mode of conflict (and crime) at societal levels, involving measures short of war, in which the protagonists use—indeed, depend on using—network forms of organization, doctrine, strategy, and communication. These protagonists generally consist of dispersed, often small groups who agree to communicate, coordinate, and act in an internetted manner, often without a precise central leadership or headquarters. Decisionmaking may be deliberately decentralized and dispersed.

Thus netwar differs from traditional modes of conflict and crime in which the protagonists prefer to use hierarchical organizations, doctrines, and strategies, as in past efforts to foster large, centralized mass movements along Leninist lines. In short, netwar is about Hamas more than the PLO, Mexico's Zapatistas more than Cuba's Fidelistas, the Christian Identity Movement more than the Ku Klux Klan, the Asian Triads more than the Sicilian Mafia, and Chicago's Gangsta Disciples more than the Al Capone Gang.

Actors across the spectrum of social conflict and crime are evolving in the direction of netwar. This includes familiar adversaries who are modifying their structures and strategies to gain advantage from the rise of network designs: e.g., transnational terrorist groups, black-market proliferators of weapons of mass destruction (WMD), drug and other criminal syndicates, fundamentalist and ethnonationalist movements, intellectual-property pirates, and immigration and refugee smugglers. Some urban gangs, rural militia organizations, and militant single-issue groups in the United States are also developing netwar-like attributes.

But that is not all: The netwar spectrum may increasingly include a new generation of revolutionaries and activists who espouse postindustrial, information-age ideologies that are just now taking shape. In some cases, identities and loyalties may shift

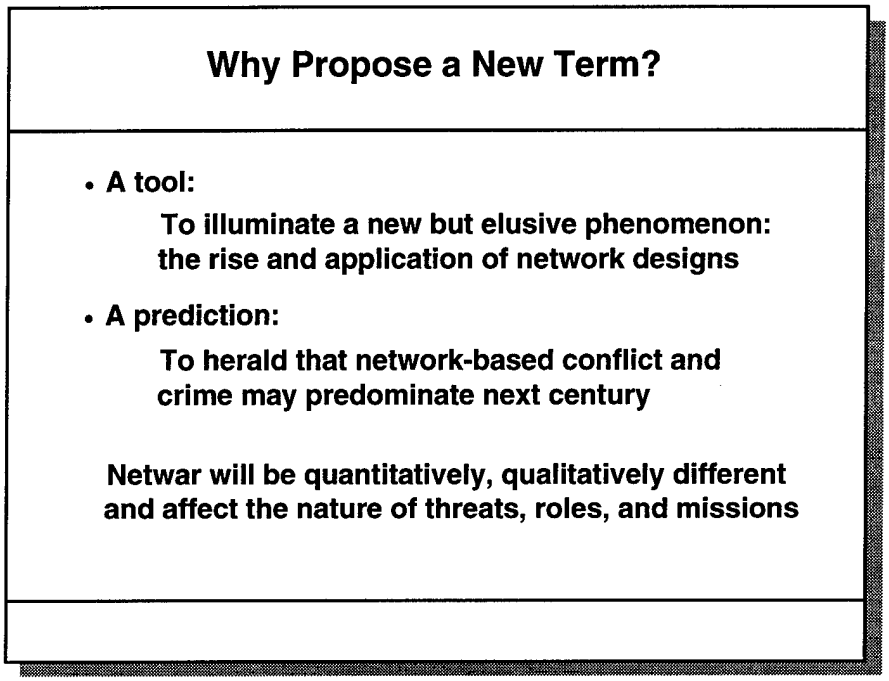
from the nation-state to the transnational level of "global civil society." New kinds of actors—e.g., anarchistic and nihilistic leagues of computer-oriented "cyboteurs"—are also beginning to arise who may partake of netwar.

Many if not most netwar actors will be nonstate and even stateless. Some may be agents of a state, but others may turn states into their agents. Odd hybrids and symbioses are likely. Moreover, a netwar actor may be both subnational and transnational in scope.

Many netwar actors may be antagonistic to U.S. interests, such as WMD proliferators. But others, like some transnational social activists, may not. In some cases, a netwar actor may benefit U.S. interests. Many variations are possible. Thus the advent of netwar may prove mainly a bane but at times a boon for U.S. policy.

The full spectrum of netwar proponents may seem broad and odd at first glance. Some actors could be fit into standard notions of LIC, OOTW, and crime. But not all fit easily into prevailing categories. And trying to make them fit risks overlooking the underlying pattern that cuts across all these variations: the use of network forms of organization, doctrine, strategy, and communication attuned to the information age.

Despite the modernity of the concept, historical instances of netwar-like actors abound. Examples mentioned in this study include: irregular warfare in North America during the French and Indian Wars, and the American Revolution in the eighteenth century; the warfare waged by indigenous Spanish guerrillas against the Napoleonic occupation in the early nineteenth century; as well as pirates and other criminals and terrorists that have long operated on the fringes of empires and nation-states. Yet, in contrast to the currently emerging examples of netwar, these early cases were forced, largely by circumstance, into netwar-like designs; these were not designs that were determined by explicit doctrine, or that could be sustained for long, or over great distances.




We think a new term is needed to focus attention on the fact that network-based conflict and crime are increasing. No current terms about LIC and OOTW fit this purpose. Moreover, the term "information warfare" (IW) and its derivatives (e.g., "infowar," "information warriors") are both too broad and too narrow to be appropriate. On the one hand, IW is used sometimes to refer to the entire spectrum of information-age conflict; on the other hand, it is increasingly associated with narrow technical issues of cyberspace vulnerability, security, and safety.

The term "netwar" connotes that the information revolution is as much about organizational design as about technological prowess, and that this revolution favors whoever masters the network form. The term amounts, then, to both a tool and a prediction:

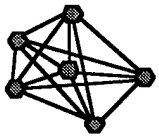
- *Tool,* because it illuminates—and instructs the eye to focus on—a new but elusive phenomenon requiring new concepts and methodologies to understand: the rise of network forms of organization.
- *Prediction,* because it heralds the prospect that networked adversaries will probably predominate the spectrum of conflict and crime early next century.

The term may strike some readers as fanciful, and a better term may yet be found. But meanwhile, in addition to providing a basis for this analysis, it is already being adopted by protagonists of varied political creeds who believe it resonates with their doctrines and objectives. For example, some extreme rightist militia members in the United States have been heard to declare netwar (or *netkrieg*) against the U.S. government, and have organized a virtual *netwaffe.* Also, center-left activists operating in Mexico sometimes refer to themselves now as "netwarriors."

The phenomenon of netwar is not entirely new—there are examples from decades past—but it is growing and spreading to an extent that will make it quantitatively and qualitatively different from what has gone before. It is becoming both more plentiful and more powerful, enough to compel a rethinking of the overall nature of potential threats, and of the roles and missions for responding to them.

## Netwar Design Elements

- **Web of dispersed, interconnected "nodes"**
  - **Nodes may be large or small in size,**
  - **tightly or loosely coupled to each other,**
  - **inclusive or exclusive in membership,**
  - **specialized or segmentary**



- **Flat structure: no central command, little hierarchy, much consultation, local initiative—a "panarchy"**
- **Central doctrine and decentralized tactics**
- **Dense communication of functional information**

**—> A distinctive design with unique strengths**

The phenomenon of netwar is still emerging; its organizational, doctrinal, and other dimensions are yet to be fully defined and developed. But the outlines are detectable.

An archetypal netwar actor consists of a web (or network) of dispersed, interconnected "nodes" (or activity centers)—this is its key defining characteristic. It may resemble the bounded "all-channel" type of network pictured above. These nodes may be individuals, groups, formal or informal organizations, or parts of groups or organizations. The nodes may be large or small in size, tightly or loosely coupled, and inclusive or exclusive in membership. They may be segmentary or specialized; that is, they may look quite alike and engage in similar activities, or they may undertake a division of labor based on specialization. The boundaries of the network may be sharply defined or blurred in relation to the outside environment.

The organizational structure is quite flat. There is no single central leader or commander; the network as a whole (but not necessarily each node) has little to no hierarchy. There may be multiple leaders. Decisionmaking and operations are decentralized and depend on consultative consensus-building that allows for local initiative and autonomy. The design is both acephalous (headless) and polycephalous (Hydra-headed)—it has no precise heart or head, although not all nodes may be "created equal." In other words, the design is a heterarchy, but also what might be termed a "panarchy" (see below).

The structure may be cellular for purposes of secrecy or substitutability (or interoperability). But the presence of "cells" does not necessarily mean a network exists, or that it is of the "all-channel" design. A hierarchy can also be cellular, as has been the

case with some subversive organizations. Or the cells may be arranged in a "chain" or "star" rather than an all-channel shape.

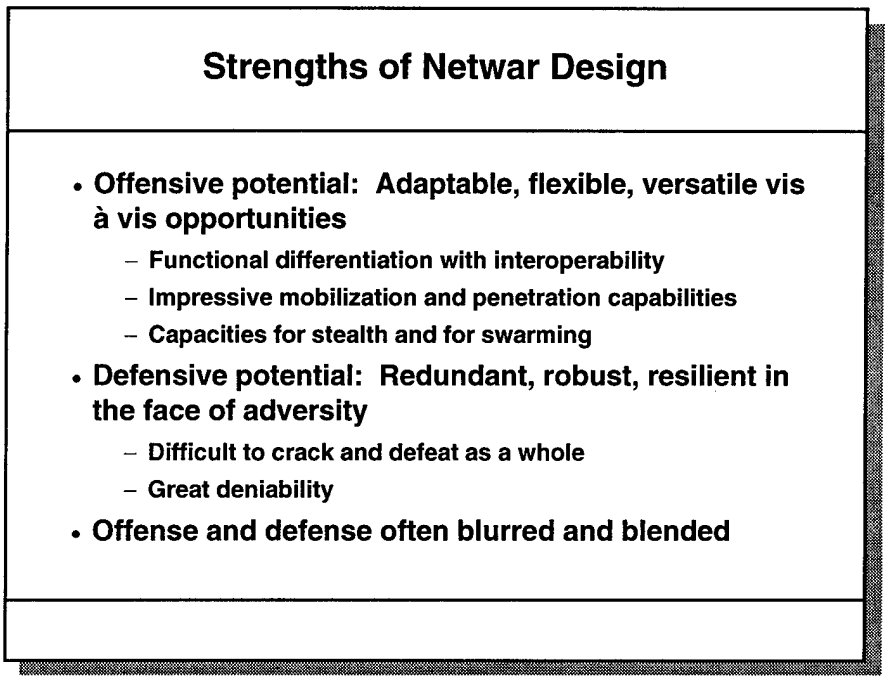
The capacity of this nonhierarchical design for effective performance over time may depend on a powerful doctrine or ideology, or at least a strong set of common interests and objectives, that spans all nodes, and to which the members subscribe in a deep way. Such a doctrine can enable them to be "all of one mind" even if they are dispersed and devoted to different tasks. It can provide an ideational, strategic, and operational centrality that allows for tactical decentralization. It can set boundaries and provide guidelines for decisions and actions so that they do not have to resort to a hierarchy—"they know what they have to do." That is why a nouveau term like panarchy may be more accurate than heterarchy.

The design depends on having a capacity—better yet, a well-developed infrastructure—for the dense communication of functional information. This does not mean that all nodes have to be in constant communication; that may not make sense for a secretive actor. But when communication is needed, information can be disseminated promptly and thoroughly, both within the network and to outside audiences.

In many respects, this archetypal netwar design resembles a "segmented, polycentric, ideologically integrated network" (SPIN). The SPIN concept, identified by anthropologist Luther Gerlach and sociologist Virginia Hine, stems from an analysis of U.S. social movements in the 1960s and 1970s:

> By segmentary I mean that it is cellular, composed of many different groups. . . . By polycentric I mean that it has many different leaders or centers of direction. . . . By networked I mean that the segments and the leaders are integrated into reticulated systems or networks through various structural, personal, and ideological ties. Networks are usually unbounded and expanding. . . . This acronym [SPIN] helps us picture this organization as a fluid, dynamic, expanding one, spinning out into mainstream society (Gerlach, 1987, p. 115, based on Gerlach and Hine, 1970).

The SPIN concept is a precursor of the netwar concept. Indeed, Gerlach and Hine anticipated two decades ago many points about network forms of organization that are just now coming into vogue.




This distinctive design has unique strengths for both offense and defense. On the offense, netwar is adaptable, flexible, and versatile vis-à-vis opportunities and challenges that arise. This may be particularly the case where there is functional differentiation and specialization among the network's nodes. These node-level characteristics, rather than implying a need for rigid command and control of group actions, combine with interoperability to allow for unusual operational flexibility, as well as for a rapidity of maneuver and an economy of force.

When all, or almost all, network elements can perform either specialized or general missions, the mobilization process can unfold rapidly. This capability alone should improve offensive penetration since the defense's potential warning time may be truncated. The capacity for a "stealthy approach" of the attacking force suggests the possibility that, in netwar, attacks will come in "swarms" rather than in more traditional "waves."[1]

Further, during the course of a netwar offensive, networked forces will, more than likely, be able to maneuver well within the decisionmaking cycle of more hierarchical opponents. This suggests that other networked formations can reinforce the original assault, swelling it; or they can launch swarm attacks upon other targets, presenting the defense with dilemmas about how best to deploy their own available forces.

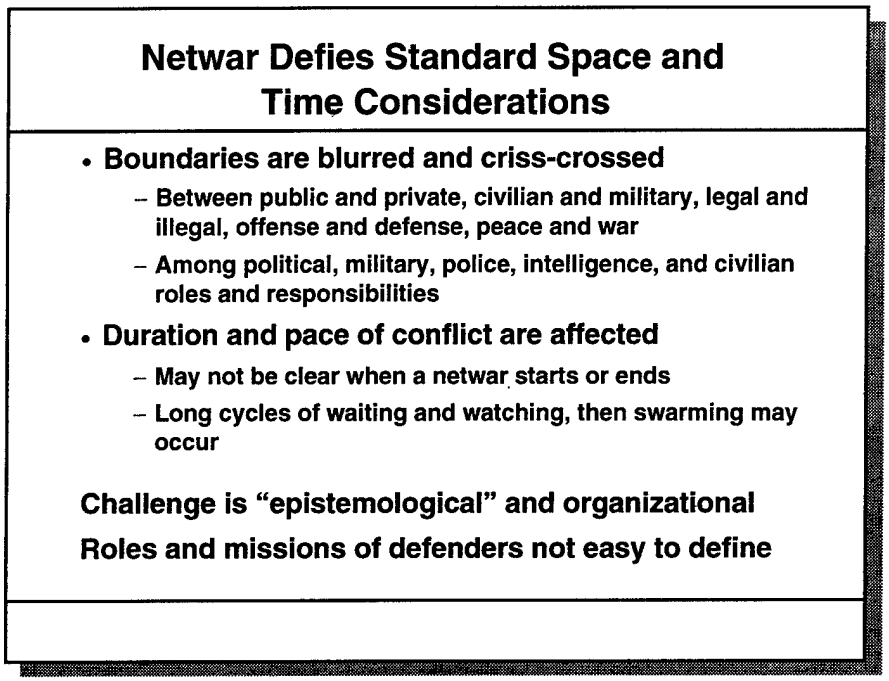
In terms of their defensive potential, networks tend to be redundant and diverse, making them robust and quite resilient in the face of adversity. Because of their capacity for interoperability, and their absence of central command and control structures, such network designs can be difficult to crack and defeat as a whole. In par-

[1]Swarm networks and the capacity of networks for swarming are raised by Kelly (1994).

ticular, they defy counterleadership targeting (i.e., "decapitation"). This severely limits those attacking the network—generally, they can find and confront only portions of it. The rest of the network can continue offensive operations, or swarm to the aid of the threatened nodes, rather like antibodies. Finally, the deniability built into a network affords the possibility that it may simply absorb a number of attacks on distributed nodes, leading the attacker to believe the network has been harmed when, in fact, it remains operationally viable and may actually find new opportunities for tactical surprise.

The difficulty of dealing with netwar actors is deepened when the line between offense and defense is "blurred"—or "blended." When blurring is the case, it may be difficult to distinguish between attacking and defending actions; they may be observationally equivalent. Swarming, for example, may be employed to attack some adversary, or to form an antibody-like defense against incursions into an area that formed part of the network's defensive zone against a hierarchical actor. A historical example is the swarming Indian attack on General George Braddock's forces during the French and Indian Wars—an instance of a network of interconnected American Indian tribes (Gipson, 1946) triumphing over an army designed around a rigid, traditional command hierarchy. While the British saw the Indian attack as presaging a major offensive against the seaboard colonies, it was but an effort to deter incursions into the French-held Ohio River Valley. The French and their Indian allies, outnumbered by the colonists and British imperial forces, took advantage of the disarray caused by their attack to engage in other pinprick raids. This reinforced the British view of an offensive in the making, compelling them to attend primarily to defensive preparations. This lengthened the time it took for the British to muster forces sufficient for the defense of the colonies and the taking of Canada (Parkman, 1884). Today, as discussed later, the Zapatista struggle in Mexico demonstrates anew the blurring of offense and defense.

The blending of offense and defense will often mix the strategic and tactical levels of operations. An example is the netwar-like guerrilla campaign in Spain during the Napoleonic Wars. Much of the time, the guerrillas, and the small British expeditionary force, pursued a strategic offensive aimed at throwing the French out of Iberia. However, more often than not, pitched battles were fought on the defensive, tactically. Similarly, where the guerrillas were on the defensive strategically, they generally took the tactical offensive. The war of the mujahideen in Afghanistan provides an excellent modern example.




This blurring of offense and defense reflects a broader feature of netwar: It tends to defy and cut across standard spatial boundaries, jurisdictions, and distinctions between state and society, public and private, war and crime, civilian and military, police and military, and legal and illegal. A netwar actor is likely to operate in the cracks and gray areas of a society.

A netwar actor may also confound temporal expectations by opting for an unusual duration and pace of conflict. Thus, it may not be clear when a netwar has started, or how and when it ends. A netwar actor may engage in long cycles of quietly watching and waiting, and then swell and swarm rapidly into action.

Moreover, sometimes it may not be clear who the protagonists are. Their identities may be so blurred, and so tangled with other actors' identities, that it is difficult to ascertain who, if anyone in particular, lies behind a netwar. This may be particularly the case where a network configured for netwar is transnational and able to maneuver adroitly and quietly across increasingly permeable nation-state borders.

This means, as Szafranski (1994, 1995) illuminates in discussing "neo-cortical warfare," that the challenge can be "epistemological": a netwar actor may aim to confound people's most fundamental beliefs about the nature of their society, culture, and government, partly to strike fear but perhaps mainly to disorient people so that they no longer presume to think or act in "normal" terms.

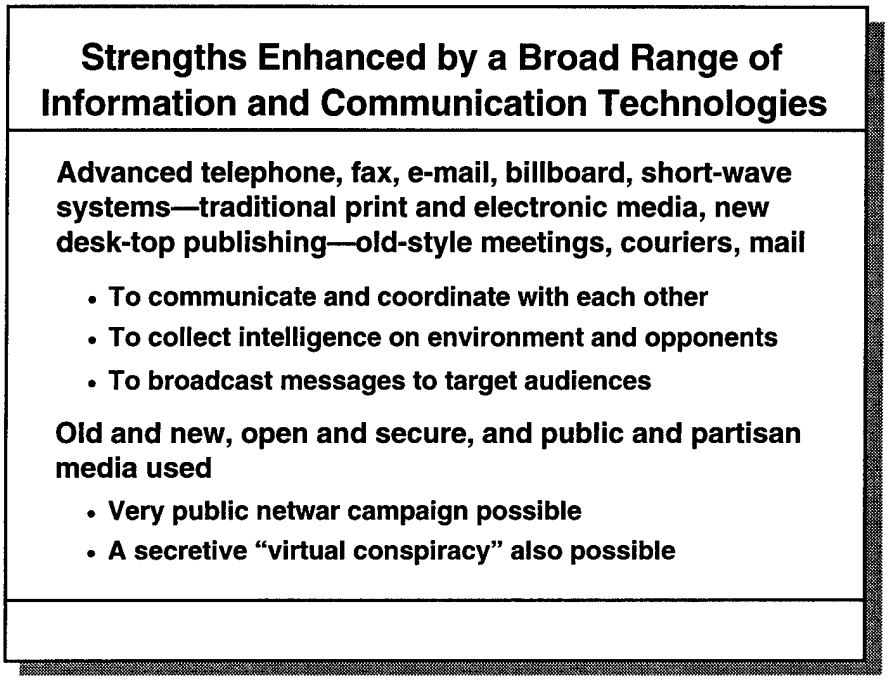
Examples can be found in the behavior of some terrorists and criminals. Terrorists, notably those using internetted, less hierarchical structures (like the "leaderless" Hamas), have been moving away from the use of violence for specific, often state-related purposes, to its use for more generalized purposes. There has been less hostage-taking accompanied by explicit demands, and more terrorist activity that

begins with a destructive act aimed at having broad but vague effects. Thus, for example, Islamic fundamentalist Sheik Rahman sought to blow up the World Trade Center with the intent of changing "American foreign policy" toward the Middle East. The current rash of domestic terrorism in the United States—e.g., the bombing in Oklahoma, and the derailment in Arizona—involves violent actions and vague or no demands. This reflects a rationality that disdains pursuing a "proportionate" relationship between ends and means, seeking instead to unhinge a society's perceptions.

Criminals also use methods tantamount to epistemological warfare when they insert themselves deeply into the fabric of their societies, e.g., by wrapping themselves in nationalism, acting like local "Robin Hoods," and/or seeking to influence, if not control, their governments and their foreign and domestic policies. Examples abound, in Colombia, Italy, Mexico, and Russia, where symbiotic ties exist between criminal and governmental organizations.

The more epistemological the challenge, the more it may be confounding from an organizational standpoint. Whose responsibility is it to respond? Whose roles and missions are at stake? Is it a military, police, intelligence, or political matter? The roles and missions of defenders are not easy to define, and this may make both deterrence and defense quite problematic.

Netwar adds to the challenges facing the "nation-state." Its traditional presumptions of sovereignty and authority are linked to a bureaucratic rationality in which issues and problems are categorized so that specific offices can be charged with taking care of specific problems. In netwar, things are rarely so clear.




It is not easy to make a multiorganizational network function well—a hierarchy is easier to run. A key reason for this is that network forms of organization generally require constant dense communications. The information revolution dramatically enhances the viability of the network form (as discussed below). Thus, the new technologies strengthen the prospects and capabilities for actors to take a netwar approach to conflict and crime.

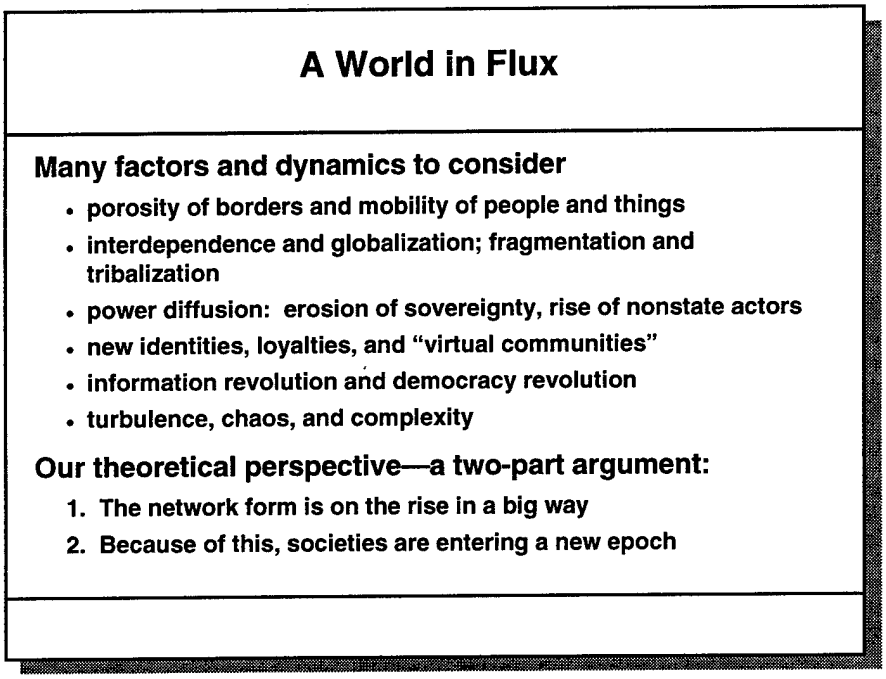
Indeed, new technologies make possible a rather "pure" variety of netwar in which all strategy and tactics—for example, disinformation campaigns and disruptive computer hacking—occur on "the Net" and in the media. But—and this should always be kept in mind—netwar is not just about the new technologies.

The latest telecommunications systems—including advanced telephone, fax, electronic mail (e-mail), and computerized billboard and conferencing systems—all contribute to netwar, and their roles in recent conflicts are often remarked about. But older technologies, like short-wave radio and cassette tape, are also important for some actors. Computerized desktop publishing, a fairly recent development, enhances the outreach of some actors, but access to traditional print and electronic media remains crucial too, depending on the actor and the audience. Meanwhile, old-style face-to-face meetings, human couriers, and regular mail have not ceased to play roles. If a terrorist or criminal sent a coded fax, this would likely be an example of netwar-related behavior, but if the same actor paid off a journalist for an article critical of some U.S. policy, this may also be an example.

Such technologies enhance the capabilities of a network's members not only to coordinate with each other, but also to collect intelligence on the external environment and on their opponents, and to broadcast or otherwise transmit messages to target

audiences. The varieties of netwar actors that we discuss later have used all kinds of old and new, high-tech and low-tech, open and secure, and public and partisan media; indeed, many netwar actors are likely to use a layered mix. The technologies can be used to wage a very public netwar campaign (as in Mexico) or to foster a secretive "virtual conspiracy" (as may be an aim of some extreme rightists in the United States).[2]

[2]Credit for the term "virtual conspiracy" is owed to journalist Lou Dolinar of *Newsday*.




Why is netwar likely? Looking for answers, we have examined diverse literatures on network theory, information theory, the evolution of societal complexity, and on trends in global political, security, and military affairs

Numerous recent writings—pick your favorite social scientists, futurists, philosophers, and commentators—attest that the world is in flux, and that myriad factors and dynamics should be considered by anyone who would make sense of current trends, possibilities, and uncertainties. This chart indicates, in no particular order, some points that have received attention:

- The increasing porosity of borders and the mobility of people and things.
- The phenomena of interdependence and globalization, but also of fragmentation and tribalization.

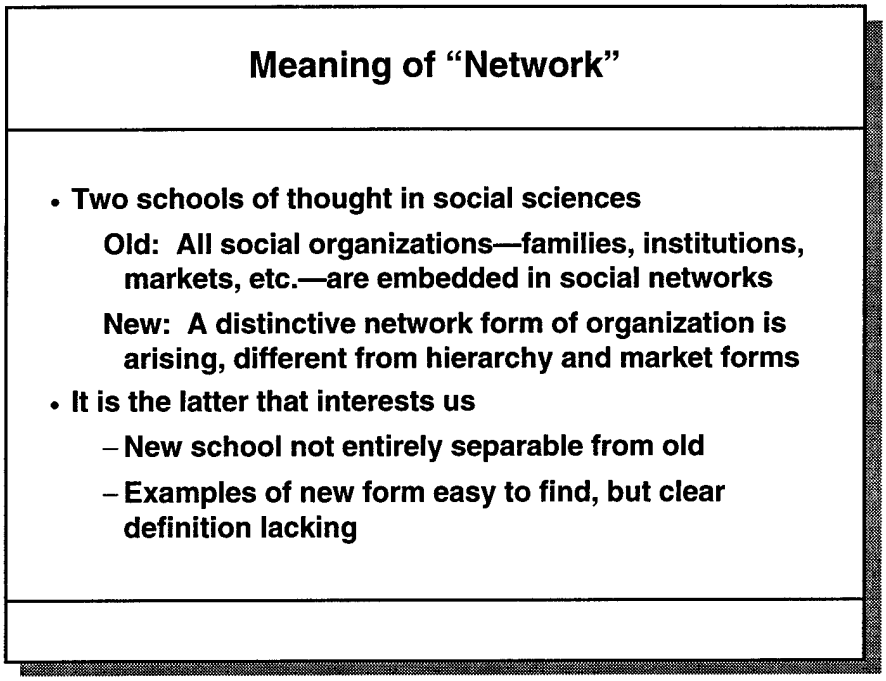
- The diffusion of power; related to that, the erosion of traditional concepts of sovereignty; and the rise of new state and nonstate actors.
- The rise of new identities, loyalties, and "virtual communities" that are not national in nature.
- The information revolution and the democracy revolution.
- The disturbing dynamics of turbulence, chaos, and complexity.

We are familiar with writings on these topics, and our views have benefited from them. Our perspective, fully elaborated, encompasses the points listed above.

Our perspective, a two-part theoretical argument, serves to explain the advent of netwar:

1. As indicated by our introductory points, the first part of our argument is that the network form of organization is on the rise, deeply affecting all realms of society. The next section elaborates on why and where the network form is on the rise and how it is likely to affect societies.
2. Because of the rise of the network form, societies are entering a new epoch of reorganization. According to our framework, four forms—the tribal, institutional, market, and network forms—underlie the organization and evolution of all societies. The network form is only the most recent to mature. Societies advance by learning to use and combine these four forms in a progression that gives rise to epochal shifts in the nature of both conflict and cooperation.

As we unfold these arguments, we identify implications for future conflict and prepare to discuss the various forms of netwar in a later chapter.




## THE RISE OF NETWORK FORMS OF ORGANIZATION

Anthropologists and sociologists have studied *social* networks for many decades. According to the most established school of thinking, basically all social organizations—families, groups, elites, institutions, markets, etc.—are embedded in networks of social relations (Granovetter, 1985; Nohria and Eccles, 1992). For this school, the network is more the "mother of all forms" than a specific type of complex organization.

Prior to the 1990s, scholarly writings occasionally appeared that treated the network as a specific, deliberate, even formal *organizational* design (e.g., Heclo, 1978; Perrow, 1979; Chisholm, 1989; also Gerlach and Hine, 1970; Gerlach, 1987). But such efforts were more the exception than the rule, and some occurred on the margins of the social sciences, including the illuminating work by Gerlach and Hine on SPINs that we quoted earlier.

Lately, and largely as a result of research by economic sociologists who study innovative corporate designs (notably Powell, 1990; and Powell and Smith-Doerr, 1994), a new school of thinking about networks is beginning to cohere. It looks beyond informal social networks to see that formal organizational networks are gaining strength as a distinct design—distinct in particular from the "hierarchies and markets" that organizational economists and economic sociologists normally emphasize:

> [T]he familiar market-hierarchy continuum does not do justice to the notion of network forms of organization. . . . [S]uch an arrangement is neither a market transaction nor a hierarchical governance structure, but a separate, different mode of exchange, one with its own logic, a network (Powell, 1990, pp. 296, 301).

This new school of analysis and the numerous examples and case studies it affords serve to validate our point that network forms of organization are on the rise and becoming more viable than ever. But the new school is mostly about economic organization. And clear, precise definitions are still lacking as to what is and is not a network.

As discussed in some detail in a later chapter, distinctions may be made among what are termed "chain," "star" or "hub," and "all-channel" types of networks. In this chapter, we focus on the all-channel type, in which all members are connected to each other and do not have to go through other members (as in a chain or hub design) to communicate and coordinate with each other.

## Why Network Forms of Organization Are on the Rise—and Where

- **Networks were once deemed an inferior way to organize, partly because they require dense communications**
- **New technologies finally provide this**
- **Thus, rise of network form is tied to the worldwide information revolution**
- **Development is in early stages, gaining impetus, and affecting actors in all realms**
  - **state actors: e.g., rise of inter-agency mechanisms**
  - **market actors: e.g, rise of web-like global enterprises**
  - **civil-society actors: e.g., rise of issue-related networks**

Despite the claims of some anthropologists and sociologists about the significance of the *social* networks they study for all manner of personal and institutional behaviors, the network as a formal *organizational* design has generally had poor standing among many economists and theorists (e.g., Williamson, 1975). Networks have long been deemed inefficient and inferior as a form of organization, especially compared with hierarchies and markets. Among other things, networks were said to require too much back-and-forth, to require "high bandwidth" communication among all members, to take too long to reach decisions, and to be too vulnerable to free riders.

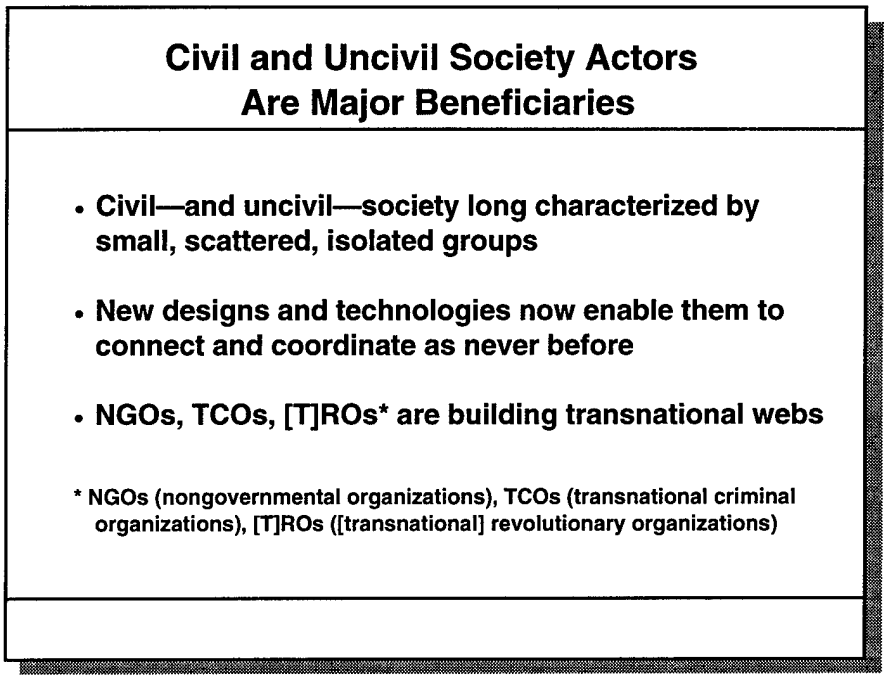
Indeed, all-channel networks do require rapid, dense, multidirectional communications to function well and endure—more so than do other forms of organization. The past limitations of this form of organization are closely tied to information and communications factors.

The new technologies—e.g., advanced telephone, fax, e-mail, computer billboard, and conferencing systems, supported by fiber-optic cable and satellite systems—finally provide the level of connectivity and bandwidth that favors all-channel organizational designs. Today, diverse, dispersed, autonomous actors are able to consult, coordinate, and act jointly across great distances on the basis of more, better, and faster information than ever before. The rise of the network form thus reflects, and is tied to, the information revolution.

The rise of network forms of organization is at an early stage, still gaining impetus. It may be decades before this trend reaches maturity. But it is already affecting all major realms of society. In the realm of the *state*, it is facilitating the development of interagency mechanisms for addressing complex policy issues that cut across jurisdictional boundaries. In the realm of the *market*, it has been facilitating the growth of

*keiretsus* and other distributed, web-like global enterprises (and so-called "virtual corporations"). Indeed, volumes are being written about the benefits of network designs for business corporations and market operations—to the point that casual (and some not-so-casual) observers might presume that this is the realm most affected and benefited.

Yet, actors in the realm of *civil society* may be the main beneficiaries. The trend is increasingly prominent in this realm, where issue-oriented multiorganizational networks continue to multiply among activists and interest groups across the political spectrum. Over the long run (as discussed in the next section), civil society is likely to be strengthened more than the other realms, in both absolute and relative terms.




What is meant by "civil society"—never a clear term—continues to evolve. Classic views, starting centuries ago, have emphasized "associations" that mediate between state and society within a nation: e.g., churches, schools, labor unions, businesses, political parties, and other voluntary groups, interest groups, professional organizations, etc. Recent views, beginning a few decades ago, do not reject the classic views but emphasize "new social movements"—such as environmental, human-rights, peace, and other movements—that are increasingly transnational in scope. Two rising indicators—listings in the *International Directory of Non-Governmental Organizations* (published since the 1970s), and subscribers to the computer networks affiliated with the Association for Progressive Communications (APC, the favored network of networks for activists since its formation in 1989)—speak to the rising importance of nongovernmental organizations (NGOs) for policy issues around the world, and the relationship between the NGOs' rise and the information revolution.

Even where civil society has been strong—as in the liberal democracies of Western Europe and North America—it has long been characterized by groups that often had to work in isolation or in fleeting coalitions and that, as a result, were weaker than state and market actors. Now, however, the new information technologies and related organizational innovations increasingly enable civil-society actors to reduce their isolation, build far-flung networks within and across national boundaries, and connect and coordinate for collective action as never before. As this trend deepens and spreads, it will strengthen the power of civil-society actors relative to state and market actors around the globe (Frederick, 1993; Ronfeldt, 1993).

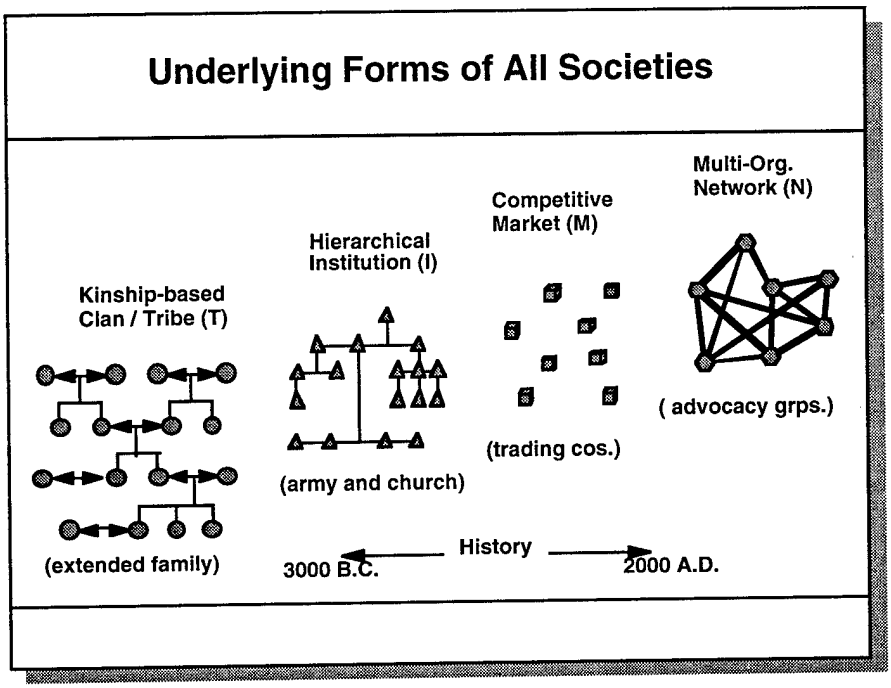
For years, a cutting edge of this trend could be found among left-leaning activist NGOs concerned with human-rights, environmental, peace, and other social issues at local, national, and global levels. Many of these rely on APC affiliates for commu-

nications and aim to construct a "global civil society" strong enough to counter the roles of state and market actors. In addition, the trend is spreading across the political spectrum. Activists on the right—from moderately conservative religious groups, to militant antiabortion groups—are also building national and transnational networks based in part on the use of new communications systems.

Not only civil society but also "uncivil society" is benefiting from the rise of network forms of organization. Uncivil actors—like criminal gangs and terrorist groups—once operated pretty much in isolation from each other. Now, transnational criminal organizations (TCOs) are taking shape (Williams, 1994, 1995). What might be termed transnational revolutionary organizations (TROs) are also emerging on the political left (e.g., Hamas) and the right (e.g., among white supremacy groups). All are building global networks as "force multipliers," and using all manner of new communications technologies to do so.

This trend—the rise of network forms of organization—is still at an early stage, but it is already a very important topic for theoretical research and policy analysis. New and interesting work can be done just by focusing on this trend. At the same time, the trend is so strong that, projected into the future, it augurs transformations in how societies are organized—if not societies as a whole, then at least key parts of their governments, economies, and especially their civil societies.

The trend thus raises questions not only about the significance of the network form itself, but also relative to other forms of organization. The rise of the network form should be analyzed partly in terms of how it is interwoven with, and related to, other basic forms of societal organization. But what are those other forms?




## THE EVOLUTION OF SOCIETIES[1]

The more we study the rise of network forms of organization, the more we think it means that societies are entering a new epoch of organization and transformation—and the more we wonder what other forms undergird the organization of societies and the nature of their actors. This takes us to the second part of our theoretical perspective.

What other forms account for the organization of societies? How have people organized their societies across the ages? The answer, in our view, may be reduced to four basic forms of organization:

- The kinship-based tribe, as denoted by the structure of extended families and clan and other lineage systems.
- The hierarchical institution, as exemplified by the army, the (Catholic) church, and ultimately the state.
- The competitive-exchange market, as exemplified by merchants and traders responding to forces of supply and demand.
- The collaborative network, as found today in the ties among some NGOs devoted to social advocacy.

[1]Much of the text in this and the preceding section is also used in Ronfeldt (1996); earlier versions appear in Ronfeldt (1993) and Ronfeldt and Thorup (1995).

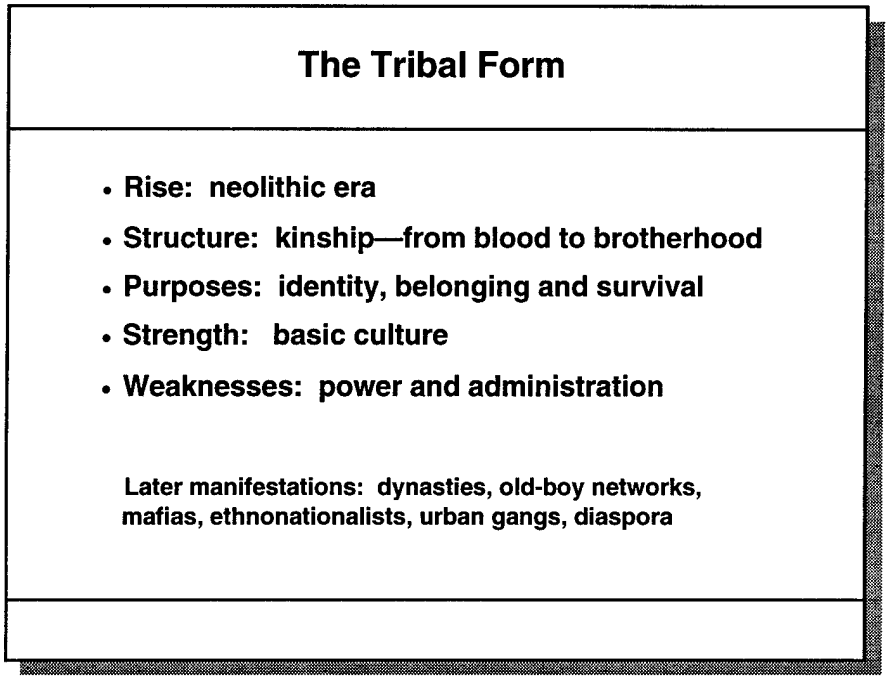
Each form, writ large, ultimately represents a distinctive system of beliefs, structures, and dynamics about how a society should be organized—about who can achieve what, why, and how.

Incipient versions of all four forms were present in ancient times. But as deliberate, formal organizational designs with philosophical portent, each has gained strength at a different rate and matured in a different historical epoch over the past 5000 years. Tribes were first, hierarchical institutions came second, and competitive markets later. Collaborative networks of the type discussed above appear to be next.[2]

The rise of each form is briefly discussed next, as prelude to assembling the four in a framework—currently called the "TIMN framework"—about the long-range evolution of societies.

---

[2]Class, which many social scientists regard as a basic form of organization, is, in this framework, not a basic form, but a result of interactions among and experiences with the four basic forms.




The first major form to define the organization of societies is the tribe, which began to emerge in the Neolithic era some 5000 years ago.[3] Its key organizing principle is kinship—initially of blood, and later also of brotherhood. Its key purpose (or function) is to render a sense of social identity and belonging, thereby strengthening a people's ability to unite and survive. The maturation of this form serves to define a society's basic culture, including its ethnic, linguistic, and civic traditions. Indeed, what happens at this level of organization has remained a basis of cultural traits well into modern periods; it also lays the basis for nationalism.

In keeping with the primacy of kinship and the codes of conduct that stem from it, the classic tribe is egalitarian—its members share communally. It is segmentary—every part looks like every other part, and there is little or no specialization. And it is "acephalous" or headless—classic tribes do not have strong, central chiefs. (The "chiefdom" is a transitional phase between tribes and early states.)

A society cannot advance far (at least not in developmental terms) with a tribal organization. It is vulnerable to clan feuds and resource scarcities, and tends to alternate between "fusion" (where clans intermarry and absorb outsiders) and "fission" (where a part hives off and goes its own way). The tribal form is particularly limited and inefficient for dealing with problems of rule and administration, as in attempting to run a large agricultural activity or govern a conquered tribe. And that takes us to the next form to evolve: the hierarchical institution.

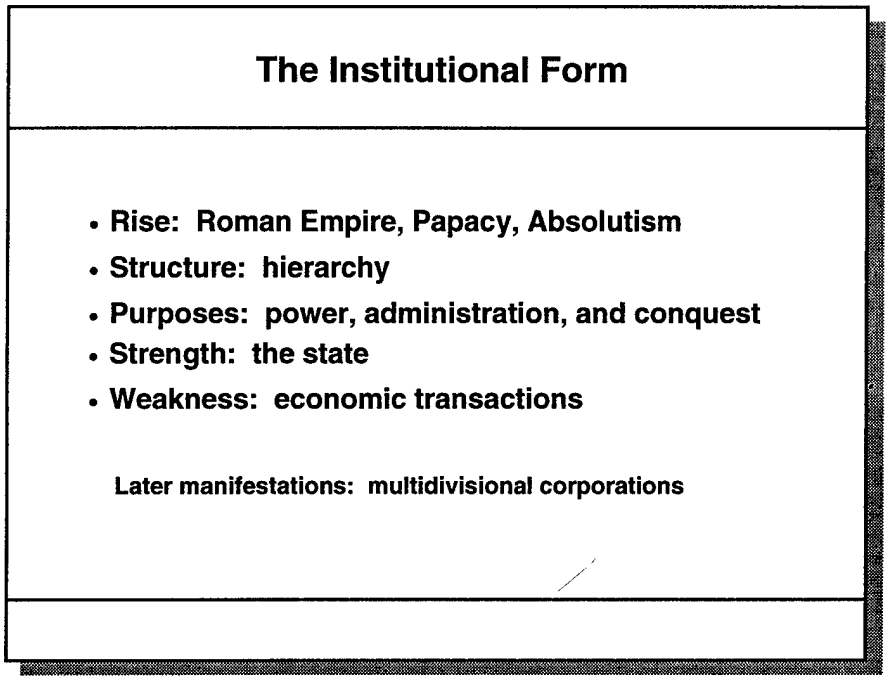
---

[3]Studies consulted include Evans-Pritchard (1940), Fried (1967), Johnson and Earle (1987), Sahlins (1968), and Service (1971).

But as we move to discuss that and later forms, the point should be kept in mind that tribe-like patterns, which once dominated the organization of societies, remain an essential basis of identity and solidarity as societies become more complex and add state, market, and other structures. This is true for societies as diverse as China, where extended family structures constantly affect all manner of political, economic, and other relations, and the United States, whose emphasis on the nuclear family and immigration from all areas of the world has resulted in an unusually loose social fabric, in which societal "kinship" often depends more on a sense of brotherhood than blood, as seen in fraternal associations.

People in many parts of the world remain—even prefer to remain—at this "stage" of development and have not effectively adopted the institutional or other forms of organization discussed below. Some of the worst ethnic conflicts today involve peoples who have lost their central institutions and reverted to ferocious neo-tribal behaviors (e.g., in the Balkans), or who fight to retain their traditional clan systems and resist the imposition of outside state and market structures (e.g., in Chechnya, Chiapas, and Somalia). Some dictatorships that seem to rest on a strong state are really grounded on a particular predominant clan (e.g., in Iraq). In the United States, urban gangs like the "Bloods" and the "Crips" in the Los Angeles area represent a recurrence to clannish brotherhoods by youths who lack strong nuclear family ties and do not see a future for themselves in the state, market, or other structures around them.

Yet, however much a set of people may enjoy the sense of solidarity and community that a tribal life-style can provide, no society or segment of society can make much progress in modern terms solely on the basis of this form.




The second form to develop is the hierarchical institution.[4] Its early high points are the ancient empires—notably the Roman Empire—and later the absolutist states where all of society was supposed to assume its place under a top-down hierarchy. A major result of this form's development is the state, which overwhelms the tribal design. The works of philosophers such as Thomas Aquinas and Jean Bodin and modern theorists such as Max Weber exemplify the concern with institutional order. Government and corporate organization charts depict what institutional systems look like.

As seen in traditional institutions such as the army, the monarchy, and the Catholic church, the essential principle behind this form is hierarchy. It enables a society, or a sector of it, to address problems of power, authority, and administration, and advance by having a center for decision, control, and coordination that is absent in the classic tribe. The hierarchical form excels at activities like building armies, organizing large economic tasks, dispensing titles and privileges, enforcing laws, ensuring successions, imposing religions, and running imperial enterprises—all activities at which the tribal form was lacking.

Hierarchical institutions are typically centralized and built around chains of command; bureaucratization occurs as they become more elaborate and technically oriented. Partly borrowing from the tribal culture, this form thrives on ritual, ceremony, honor, and duty, especially where aristocratic dynasties take hold. Yet, this form involves a new rationality. As Weber spelled out, the development of legitimate, authoritative institutions to rule a society involves, among other things, administrative

[4]Studies consulted include Claessen and Skalník (1978), Cohen and Service (1978), Poggi (1978), Service (1975), and Tainter (1988).

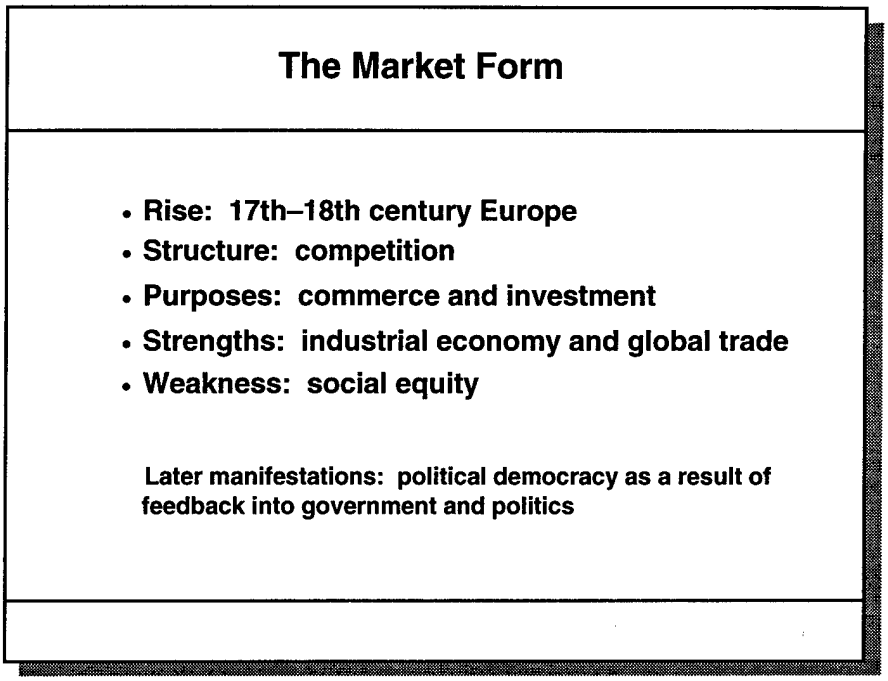
specialization and differentiation, professionalization of office cadres, the replacement of ascriptive by achievement criteria, and the development of sanctioned instruments of coercion that spell an end to the egalitarianism of the tribal form. Rulers claim sovereign rights to build empires and nation-states.

War and religion proved great rationalizers of hierarchy. For example, in Europe, following the collapse of the Roman Empire, the Catholic Church became the most powerful hierarchy, while under various monarchies the army (or armies) developed as the core agency of the future nation-state. As the two hierarchies—church and state—vied to dominate all manner of political, economic, social, and other affairs, they came into conflict. By the seventeenth century, the state had pushed the church aside, and the nation-state became the dominant actor in Europe—a trend that culminated in the Treaty of Westphalia ending the Thirty Years' War.

Eventually, new concepts of citizenship and individual rights emerged to challenge the regimes of feudalism and absolutism. Additional concepts also arose about the separation and balancing of powers, federation and confederation, elections, and the rule of law, all leading to a loosening of hierarchical designs and the emergence of liberal democratic institutions. Nonetheless, the basic patterns of hierarchy persist into the modern era, whether a society and its institutions come to be called democratic or autocratic, individualist or collectivist, or by other names.

Two points bear emphasis to conclude this sketch. First, history speaks to the impossibility for a single hierarchy to rule an increasingly complex society and all its political, economic, and other affairs indefinitely. But rival hierarchies—for example, church and state—may coexist, if they define bounded realms and stay out of each other's terrain.

Second, the hierarchical design proves to have a key limitation—it cannot process complex exchanges and information flows very well. This shows up most in the area of economic transactions, which become too complex for monarchies and their bureaucracies to control in detail. They have ever greater difficulty dictating terms and prices in a productive and acceptable manner. This proves particularly the case with long-distance trade; as it grows, traders and merchants who had operated at the behest of the state work to break free of autocratic controls and go independent. Thus, the institutional paradigm of governance begins to fail in the economic realm, and gives way to the rise of the next form: the market.




That takes us to the third major form to mature: the competitive market.[5] There were marketplaces in ancient times (e.g., the Greek *agora*), but "the market" as a philosophical and organizational concept does not arise until the eighteenth century and the eve of the industrial revolution, when the writings of Scotland's Adam Smith and the French *Physiocrats* explain that a market economy will function as a self-regulating system if left alone by the state (as well as by big business monopolies). Then we see a transition in Europe from mercantilism, where the state tries to dominate the market, to capitalism, where market actors may try to dominate state actors—and in the process, mercantilism is outperformed. We also see a separation of the state and market realms, and of the public and the private sectors.

Compared with the tribal and institutional designs, the market engages a very different, even contradictory set of principles. Its essential principle is open competition among private interests that are supposed to behave freely and fairly. Its strength is that it can enable diverse actors to process diverse exchanges and other complex transactions better than can the tribal and hierarchical systems. This happens to be appropriate for trade, commerce, and investment; and the result is the market economy. At its best, this form leads to a productive, diversified, innovative economy, overcoming the preferences of the prior forms for collectivism and statism.

Whereas the ideal institutional system was hierarchical, the ideal market system is competitive and quite atomized. The new concept meant that property, products, services, and knowledge could be traded across great distances at terms and prices that reflected local exchange rates rather than the dictates of distant rulers. It meant

[5]Studies consulted include Braudel (1982), Heilbroner (1967), Hirschman (1977), North (1981), and Polanyi (1944).

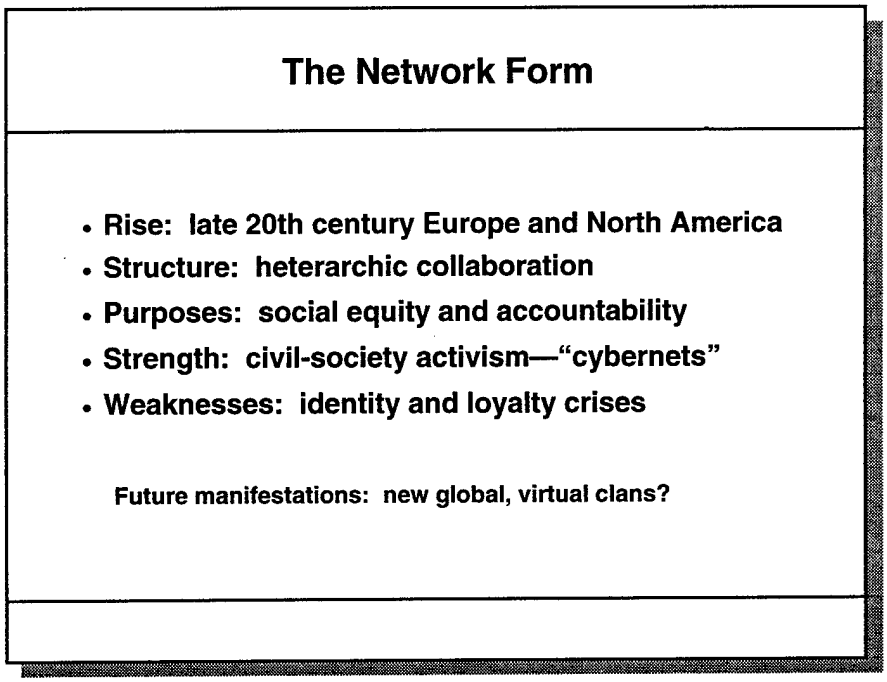
that people were entitled to act in terms of personal interests, profit motives, and individual rights that ran contrary to traditional notions of hierarchy. Thus, the market concept entailed new ideas about how a society should be organized.

Market principles were not meant to replace institutional ones. Indeed, the market system absorbed from the state some institutions that had been engaging in commerce and finance at the state's behest, like banks and trading companies. The market also rests on contractual and other laws set by the state. However, the market system involves new principles for relating specific institutions to each other. In a hierarchical system, there should normally be only one of each specific institution—e.g., a society should not have more than one army or finance ministry. But in a market system, multiple competing actors may be the norm—there can be many banks and trading companies.

While the market was not supposed to supplant the institutional system, it does displace it from its dominant position. It limits that system's scope of activity and confines it to a particular realm: the state. Yet the point to emphasize is not that of competition and conflict, but of combination. A society's ability to combine these distinctive forms of governance, many of whose principles contradict each other, renders an evolution to a higher level of complexity. It also expands a society's capabilities; for the growth of the market system strengthens the power of the states that adopt that system, even as it ensures that the state alone cannot dictate the course of economic development. Indeed, the advent of the market system, and the feedback of market principles into the realm of the state, allows for the development of political democracy, our most valued governance system today. As Charles Lindblom once wrote (1977, p. 116),

> However poorly the market is harnessed to democratic purposes, only within market-oriented systems does political democracy arise. Not all market-oriented systems are democratic, but every democratic system is also a market-oriented system.

Despite all its strengths and contributions to the advance of society, the market system has a key limitation of its own: It contributes to creating social inequities and does not prove adept at addressing them. As was the case with the earlier forms, the sharpening and the recognition of this limitation takes us to the next form to arise.




The tribal, institutional, and market forms—and their combinations—have long ruled the organization and advance of society. Some analysts have thought that this spells the end of the story. But as discussed earlier, yet another form is arising around the world: the information-age network.[6]

Its key principle is heterarchic collaboration among members who may be dispersed among multiple, often small organizations. Network designs have existed throughout history, but multiorganizational designs are now able to gain strength and mature because the new communications technologies allow small, autonomous, dispersed groups to coordinate and act jointly across great distances as never before.

While the network form is affecting all realms, civil society appears to be its home realm, the one that will be strengthened more than any other—either that, or a new, yet-to-be-named realm may emerge from it. The network form seems particularly well suited to strengthening civil-society actors whose purpose is to address social issues. At its best, this form may thus result in vast networks of NGOs geared to addressing and resolving social equity and accountability issues that actors identified with the other forms tend to ignore or are unsuited to addressing well.

The case for this view is deepening. Studies by various scholars show that an "associational revolution" is well under way, creating a nonprofit, service-oriented "third global sector"—a "social sector"—alongside the established public and private

[6]Studies consulted include Chisholm (1989), Nohria and Eccles (1992), Powell (1990), and Powell and Smith-Doerr (1994) on network organizations; Shils (1991) and Walzer (1991) on the traditions of civil society; and Drucker (1993, 1994), Frederick (1993), Kumon (1992), Salamon (1994), Spiro (1995), Thorup (1991, 1993, 1995), and Wapner (1995) on the rise of civil-society actors who are networked. Rothschild (1995) sounds a cautionary note about the "civil society strategy."

sectors. Around the world, a "global civil society" is taking shape, giving rise to "citizen diplomacy" and "world civil politics." As for the United States, according to Peter Drucker (1993),

> the post-capitalist polity needs a "third sector," in addition to the two generally recognized ones, the "private sector" of business and the "public sector" of government. It needs an autonomous social sector.

While classic definitions of civil society often include political parties and private businesses, this is less the case for new definitions. The separation of "civil society" from "state" and "market" realms may be deepening.

As these trends grow, civil-society (or the new realm's) actors should gain power relative to state and market actors at local through global levels in the coming decades. While some writers claim that this will diminish the power of nation-states, the TIMN framework implies that the state, as the home of the hierarchical form, is an enduring, essential entity for a society. The state may grow even stronger in some respects (Arquilla and Ronfeldt, 1996; Skolnikoff, 1993). The key is for governmental and nongovernmental actors to learn to cooperate better. This will help strengthen the state; but it may also mean that "nations" become as well represented as "states" in policymaking processes (Thorup, 1995).

In other words, the TIMN framework recognizes a dynamic in which the rise of a new form (and its realm) reduces the scope of an existing form (and realm), yet strengthens the latter's power within that reduced scope. This was the case with the rise of the market system—it constrained the state, yet enhanced the state's power. The presumption here is that this pattern will recur with the rise of the network form.

A big question is, What will the new realm consist of? We have focused on activist NGOs devoted to social issues, but there may be additional actors. Since a new realm absorbs some actors from existing realms, is it possible that the new networks may take health, education, and welfare actors away from the state and market realms?

While this may prove all to the good, the "cybernets" of the future may, like prior forms, have inherent limitations. Indeed, their global agendas could undermine peoples' traditional loyalties, inducing a return to the problem of how people conceive of their tribal identities.

## The Forms Compared

| | CLANS / TRIBES | INSTITUTIONS | MARKETS | ORG. NETWORKS |
|---|---|---|---|---|
| KEY ERA | primitive | agricultural | industrial | postindustrial |
| KEY REALM | family / culture | state / government | economy | civil society? |
| KEY INTEREST | identity | power / authority | wealth | knowledge / info.? |
| KEY VALUE | belonging | order | freedom | justice? equity? |
| KEY RISK | nepotism | corruption | exploitation | deception? |
| KEY PRODUCT | household goods? | public goods | private goods | collective goods |
| MOTIVATION | survival | higher-authority | self-interest | consensus |
| LIMITATION | command decis. | commercial control | social equity | info. overload? |
| STRUCTURE | acephalous | hierarchical | atomized | web-like / nodal |
| | organic? | centralized | <----------> | decentralized |
| OF SPACE | circles in circles | vertical | <----------> | horizontal |
| OF TIME | cyclic (myth) | past (tradition) | present (demand) | future (needs?) |
| OF ACTION | solidarity | command / control | exchange / trade | consult / coord. |
| ARCHITECTURE | labyrinth | pyramid | atoms | "Bucky ball" |
| BODY METAPH. | skin / look | skeletal system | circulatory sys. | sensory sys. |
| INFO. TECH. | glyphs, symbols | writing, printing | teleg., telephone | digital communic. |

The chart above offers a comparative summary of many points that have been made (plus some not made) about the four forms of organization. In highlighting the distinctive attributes of each form, the table helps to show that what one is good at, another may not be. The table indicates both the strengths and weaknesses, the contradictions and potential compatibilities among the forms.

It should be evident from the chart and the preceding discussion that each form, once it is writ large and subscribed to by many actors, is more than a mere form: It becomes a system. Each form embodies a distinct cluster of values and norms; and these must be learned and must spread if a form is to take root and a realm to grow around it. Each spells an ideational and structural revolution. Each involves a set of interactions or transactions powerful enough to define a distinct realm of activity, or at least its core. Each lays the basis for a governance system that is self-regulating, and self-limiting. What is "rational"—how a "rational actor" should behave—is different in each system; no single "utility function" suits all systems.

Albert Hirschman's (1977) study about a motivational shift in Europe from political and religious "passions" to capitalist "interests" centuries ago attests to this, as does Jane Jacobs' (1992) study about the "guardian" and the "commercial" syndromes as moral "systems of survival." Moreover, E. E. Evans-Pritchard's (1940) classic on the Nuer tribe illuminates how distinctive values and norms shape social, economic, and political life in a segmentary lineage system.

Each form is thus associated with high ideals as well as new capabilities. And as each develops, it enables people to do more than they previously could. The chart indicates this. But it should also be pointed out that the forms are ethically neutral—as neutral as technologies—in the sense that they have both bright and dark sides, and

can be used for good or ill. The tribal form may breed a narrow clannishness, persisting even in advanced societies, that can justify anything, from nepotism to murder, to protect and strengthen a clan and its leaders. The institutional form can lead to dictatorial, corrupt, arbitrary hierarchies. The market form can allow for unbridled, unproductive speculation, and the rigging of market sectors to protect powerful capitalists. The network form can strengthen "uncivil society" by enabling subversive groups to mount deception campaigns, or criminal syndicates to smuggle drugs, arms, or migrants. In other words, it is not just the bright sides of each form that foster new value systems and shape new actors; the dark sides may do so as well. As Jacobs (1992) observes, "monstrous moral hybrids" are possible.

Finally, we would call attention to the bottom two lines of the chart. The first proposes that each form corresponds to a biological metaphor: tribes to the skin or the look of a body; institutions to its skeletal and muscle system (as Hobbes implied); markets to its cardiopulmonary circulatory system (as Marx noted); and networks to the sensory system. Yes, there is an evolutionary, even Darwinian presumption here.

The final line indicates that the rise of each form may be associated with a different information revolution: the tribal form with early language and writing; the institutional form with penned script and the printing press; the market system with electrical technologies like the telephone and the telegraph; and the new network form with computerized technologies. We made a point earlier about how the rise of the network form is a result of today's information revolution. Here, we clarify that the rise and the spread of each form has depended on an enabling information technology revolution that also becomes an organizational revolution (Ronfeldt, 1996).

## Societies Advance by Combining These Forms

- **T, I, M, N forms enable organization, governance of societies**
- **There is a natural progression to the emergence and combination of the forms and their realms**
- **A society's advance depends on its ability to incorporate and combine these forms**

The T, I, M, and N forms, then, appear to be the basic forms that underlie, indeed enable, the organization and governance of societies. Each form is good and useful for something; each does something better than any other form can do.

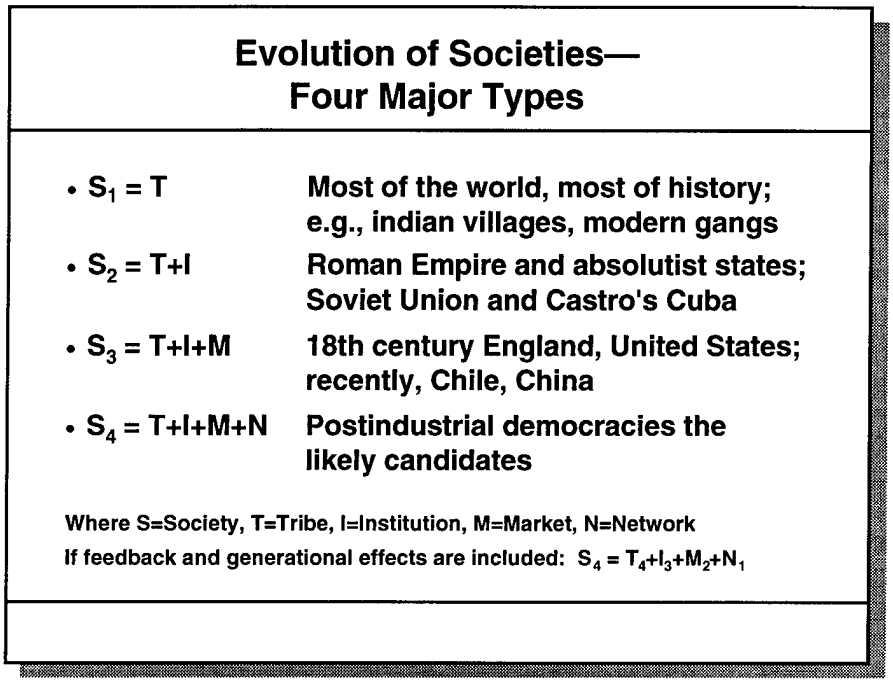
All four forms have existed since ancient times, but each has developed and matured at a different rate since then. There appears to be a natural progression to their emergence and combination. And this appears to owe mainly to the ability of each form to respond, in turn, to a key problem (or function) that societies must face and resolve as they advance. The tribal form serves to resolve primordial problems of belonging and identity; the institutional form, problems of power, authority, and administration; and the market form, problems of increasingly complex economic exchanges. What problems the network form may be best suited to resolve are not so clear; but the prior forms have generated and failed to resolve many social—especially social equity and welfare—problems, and that seems to be a major part of the answer.[7]

While this presentation has approached each form separately, the main point is that societies advance by combining them in sequence. In the end, what matters is how the forms get added and how well they function together. They are not substitutes for each other. Historically, a society's advance—its evolutionary progress—depends on its ability to use the four forms and to combine them (and their resulting realms) into a functioning whole. Societies that achieve a new combination become more powerful and more capable of complex tasks than societies that do not. A society's leaders may try to skip or deny a form (the case with Marxist-Leninist revolutionaries

[7]Chris Kedzie points out that the TIMN progression resembles Abraham Maslow's "hierarchy of needs" (Maslow, 1987).

who opposed the market form), but any success ultimately proves futile and temporary.

In other words, a comprehensive framework about societal evolution can be discerned around these four forms. Scholars, using other terms, often study societal transitions from one form to the next, typically emphasizing the time- and place-bound features of the transition they study. Keen phrases—like "the Great Divide" (Service, 1975) between tribes and early states, and "the Great Transformation" (Polanyi, 1944) wrought by the advent of capitalist market systems—may encapsulate the significance of a particular transition, implying that a new system has replaced an old one. The specifics of each transition are important, and the TIMN framework accepts this. At the same time, the framework argues that all the forms and the transitions can be assembled into a single framework. Moreover, the TIMN framework views the evolution of "complexity" as largely an additive, cumulative, or combinatorial process in which a society is able to develop various subsystems (realms) that operate according to different principles. The framework is as much about old forms persisting as it is about new forms arising. Other writers are coming to similar conclusions (parallel thinking appears in Hannerz, 1992; Kumon, 1992; Toffler 1970).




The argument may be summarized as a few simple equations in which "$S_n$" refers to societies of the first, second, third, and fourth types, and T, I, M, and N refer to tribes, institutions, markets, and networks respectively:

- $S_1$ = T —as seen in most of the world and most of history (e.g., Indian villages and modern gangs).
- $S_2$ = T+I —as epitomized by the Roman Empire at its height, by the absolutist states of the 16th century, and in this century by the Soviet Union and Castro's Cuba.
- $S_3$ = T+I+M —as exemplified by England and the United States since the 18th century, and recently by countries like Chile, China, and Mexico that have moved to develop market economies.
- $S_4$ = T+I+M+N —with the postindustrial democracies in North America and Western Europe being the most likely candidates.

These are not formal equations; they should be read more as depictions than mathematics. In the future, an effort will be made to refine the formulas for, among other uses, the purpose of comparing societies and subsocietal actors that combine or blend aspects of these forms; but work remains to be done on how best to do so and on what attributes and indicators to specify for each form and its interactions with other forms. The framework must accommodate the fact that the nature and content of a form may vary from society to society; for example, the T form is very different in Japan than in the United States. Moreover, as a note on the chart indicates, the equations should reflect the feedback effects that may occur with the addition of a new form.

Meanwhile, these depictive formulas speak to the following point: Over the ages, societies organized in tribal (T) terms are outperformed by societies that also develop institutional (I) systems to become T+I societies, often with strong states. In turn, these get superseded by societies that allow space for the market form (M) and become T+I+M societies. Now the network (N) form is on the rise, evidently with special relevance for civil society (or a new realm emerging from it). We are entering a phase of societal evolution in which T+I+M+N societies will emerge to take the lead. To do well in the 21st century, an information-age society must embrace all four forms—and these must function well together despite their contradictions.

This is not an easy progression for any society, since each step is bound to induce a vast rebalancing of societal forces. Every society has to move at its own pace and develop its own approach to each form and combination, in a process that requires modifying the older to adapt to the newer forms (and realms). Some societies have great difficulty proceeding through the progression; others prove more adaptable. Yet, despite the uniqueness of each case, in general it appears that the four forms lie behind the evolution of all societies—East, West, North, and South. All major political designs and ideologies—the "isms" and "ocracies" of world history—appear to fit the framework. Major "isms" (like feudalism and capitalism) and "ocracies" (like theocracy and democracy) generally reduce to particular combinations of, and variations on, these four generic forms.

The emergence of +N societies, and the effects of +N forces on all societies, mean that new political systems and ideologies will come to the fore in the decades ahead. Better democracies are a likelihood among the advanced nations, but new kinds of authoritarian and totalitarian regimes are also possible in retrograde situations (Ronfeldt, 1992).

These are sweeping generalizations. A full layout of the TIMN framework would have to clarify them. It would also posit a set of propositions about the dynamics embedded in the framework, as presently understood—e.g., that a form's rise is likely to have subversive effects before it has additive ones, or that a balance among the forms is best for a society's evolution. Indeed, while each transition from T through N is special, the framework implies that every form's rise sets in motion systemic dynamics that are similar for all transitions—that is, some dynamics repeat each time a new form rises. This is being worked on (Ronfeldt, 1996). Our limited objective here is to outline the TIMN framework to raise some implications for understanding the advent of netwar. We move to those implications in the next few charts.

## Patterns of Conflict and Cooperation Undergo Epochal Shifts

- **Rise of each form generates new actors, interests, issues and ideas, leading to epochal struggles**
- **Major periods of peace—and war—are associated with rise and stabilization of each form**
  - **Pax Romana**
  - **Pax Britannica**
  - **Pax Americana continues?**
- **New generation ahead: state vs. nonstate actors and nonstate vs. other nonstate actors?**

Propositions about the future may be discerned by finding patterns that reappear with each progression from T, to T+I, to T+I+M societies. It is presumed that such patterns will recur in the progression to T+I+M+N societies. Here we briefly mention a set of patterns that concern conflict.

It is often difficult—it takes decades or longer—for a society to incorporate a new form of organization. The values, norms, and "spaces" favored by one form tend to contradict those favored by another; these contradictions must be worked out for successful combination to occur. In the meantime, the rise of a form generates new kinds of actors, interests, issues, and ideas in a society. As all sectors try to adjust to the new forces and new realities, the transition from one combination to the next induces systemwide transformations and epochal philosophical, ideological, and other conflicts for some time, even though new patterns of cooperation ultimately ensue.

A society may become distorted or be torn apart as it adapts to a new form. For example, many T+I societies resist the transition to T+I+M. The great revolutions of the 20th century—the Mexican, Russian, Chinese, and Cuban—occurred in T+I societies where clannish and hierarchic structures were under stress from the infusion of capitalist practices that did more to reinforce the old structures than pave the way for a market system. Failing to make the transition to T+I+M societies, they reverted violently to T+I regimes that, in all but Mexico's case, converted absolutism into totalitarianism. Today, to varying degrees, these four nations are trying anew to make the same +M transition—testimony to the proposition that the progression is natural and cannot be avoided if a society is to advance.

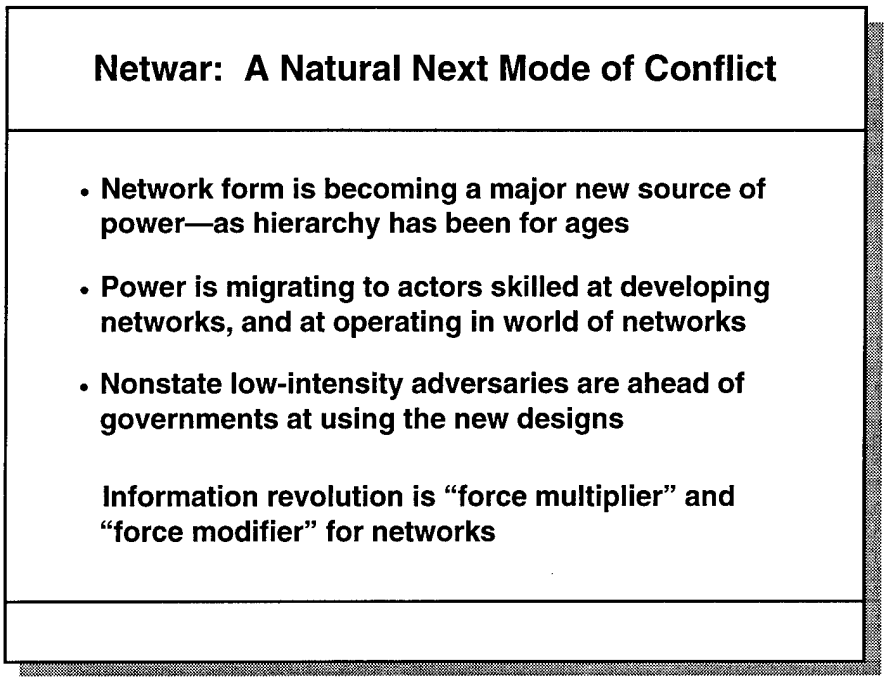
Liberal democracies emerge only from the T+I+M combination. Today, some advanced democracies, notably Canada and the United States, have begun a transition

to the +N combination, at a time when their T, I, and M elements are under stress for many reasons (family breakups, religious divisions, ethnic and racial tensions, perceived failures of government institutions and political parties, and persistent economic inequities). This explains some of the social turbulence in the United States, where many internetted single-issue groups are pitted against teach other, notably over abortion. This also helps explain the volatility of conditions in nations, like Mexico, that are moving to develop T+I+M system in parts of the world that are rife with +N forces and their spillover effects.

Whoever succeeds at making a new combination first and best stands to gain advantages over competitors. Major epochs of peace—and war—appear to be associated with the rise and stabilization of a new form in what becomes the hegemonic society of the time. Thus, the institutional revolution wrought by the T+I combination led to the preeminence of the Roman Empire—and the Pax Romana. The seminal exemplar of the +M combination, Great Britain, imposed the Pax Britannica, which transmuted into the Pax Americana as Britain declined and the second great exemplar of the +M combination, the United States, gained superpower status.

Who will create the next great Pax? Will it be whichever nation-state (or other entity?) reconfigures itself to achieve the T+I+M+N combination in time to become a hegemonic power? Or will peace in a heavily networked world not depend on there being a hegemonic actor? The answer may turn largely on which government (or other entity) works most effectively with internetted nonstate actors to project power and presence abroad. Since the world may still consist largely of contentious T, T+I, and T+I+M actors, power and presence abroad, in new as well as traditional ways, will surely remain an abiding concern of +N actors.

In any case, the advent of T+I+M+N societies and the general effects of +N forces on all societies means that a new generation of societal conflicts is in the making and will expand for decades. It will not only pit states against states, but also increase conflict between state and nonstate actors (Greenpeace-led resistance to French nuclear testing in the Pacific is a sign of this). More to the point, it will increase conflict between nonstate and other nonstate actors. In some instances, a nation-state may be more a playing field or a battleground than a central participant in such a conflict (e.g., Colombia vis-à-vis the drug cartels; Zambia as an arena of conflict between transnational poachers and the Wildlife Fund). Furthermore, the framework implies considerable conflict between societies (and parts of societies) at different stages in the TIMN progression—a point similarly made by Alvin and Heidi Toffler (1993) in their ideas about conflicts between actors who represent different "waves" of development.




In short, netwar is a natural next mode of conflict and crime. According to what we have argued so far, the advent of netwar is a result of the rise of network forms of organization, which in turn is a result of the information revolution. Not all conflicts will involve netwar—many traditional modes of conflict and crime will persist. But netwar is already ascendant.

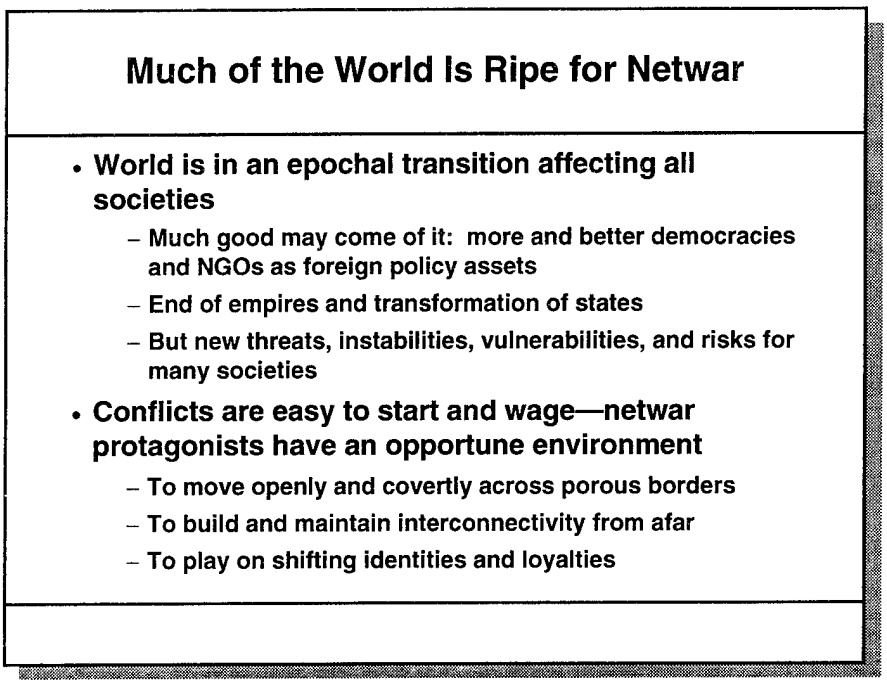
A few propositions we pose to wrap up this section are as follows:

- Organization, and knowing how to organize, have always been a source of power, independently of the resources and skills available in an organization. Today, the network form is fast becoming a major new source of power—as hierarchy has been for ages. It is especially a source of power for actors who have previously had to operate in isolation from each other, and who could or would not opt to coalesce into a hierarchical design.
- Power is migrating to actors who are skilled at developing networks, and at operating in a world of networks. Actors positioned to take advantage of networking are being strengthened faster than actors embedded in old hierarchical structures that constrain networking. This does not necessarily favor actors on any particular part of the political spectrum—it favors whoever can master network design elements.
- Nonstate adversaries—from warriors to criminals, especially those that are transnational—are currently ahead of government actors at using, and at being able to use, this mode of organization and related doctrines and strategies. It takes skill to use this mode well, but the ease of entry and the anonymity afforded by network designs also imply that we should expect an increasing "amateurization" of terrorism and crime. It is increasingly easy for protagonists to

construct sprawling networks that have a high capacity for stealthy operations by lone individuals or small groups, as well as for rapid swarming en masse.

Information is considered a "force multiplier" (notably during the Persian Gulf War, to the benefit of U.S. forces). Yet, it is important to realize that it is also a "force modifier." That is, taking full advantage of the information age—the technological and organizational innovations signified by the information revolution—is bound to require major modifications in how forces are organized and deployed for offensive and defensive operations. More to the point, as elaborated later, the use of force is likely to be focused on *disruption* rather than destruction.

Analysis of the network form provides a useful way to understand the advent of netwar—why and how the world is giving rise to a new mode of conflict. A lot can be done just by improving our ability to study this form, its levels of analysis (i.e., the organizational, doctrinal, technological, and social levels, as discussed below), and the implications for society and security. Better theories and methodologies are needed regarding how networks operate, and how they should be analyzed.



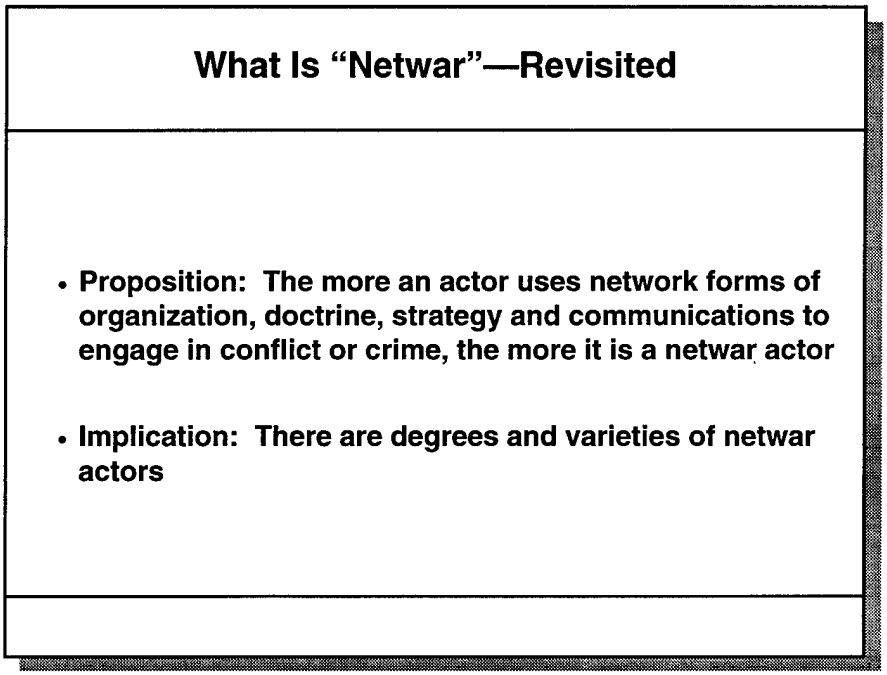

Our theoretical perspective shows that network forms of organization are on the rise—and thus that netwar is a natural next mode of conflict. It also shows that societies around the world are entering a new epoch of evolutionary change—and thus that much of the world is ripe for netwar. This may be particularly the case for advanced societies like the United States.

The TIMN framework implies that much good will come from the growth of +N forces and +N societies. More and better democracies are a distinct possibility around the world. Transnational NGOs, and the ability of such NGOs and governments to work with each other, should become a major foreign policy asset for democratic societies. Indeed, as noted earlier, "states" and "nation-states" may continue to do quite well in the new epoch. What may be coming to an end, if anything, is not the state or the state system, but rather the empire and imperialism in their classic forms. At the same time, a new model of the state may emerge, probably one that is leaner, yet draws new strength from enhanced abilities to act in concert with nonstate actors. In this vein, Drucker (1993) argues that the classic nation-state metamorphosed into the unwieldy "megastate" of the 20th century by taking on excessive social, economic, and military duties, and concludes that success in the post-capitalist age will require a different model. Other thinkers are also proposing that what lies ahead is not the demise but the transformation of the state (Arquilla and Ronfeldt, 1996).

Despite the positive side of this restructuring, new threats, instabilities, risks, and vulnerabilities lie ahead for many, if not most, societies around the world. Closed societies will continue having difficulty dealing with the information revolution and its subversive impetus for openness; the price of repression should rise as intercon-

nectivity increases. Open societies may also be increasingly at risk. Their very openness, their exposure and connectivity to the world at large, creates vulnerabilities to netwar.

The nature of the global transitions now under way means that conflicts will be relatively easy to start—and wage. Netwar protagonists face an opportune environment in many parts of the world. Among other things, they can move openly and covertly across increasingly porous borders. They can easily build and maintain the interconnectivity of their networks from afar. And they have many opportunities to play on shifting identities and loyalties, especially national ones. Finally, the very backwardness of some states, measured in terms of their low connectivity to their own societies as well as to others, may make them less vulnerable to counternetwar, perhaps increasing their incentives for starting netwars in the first place.




To reiterate: In ideal form, a netwar actor exists in (or as) a network of small, diverse units—perhaps even as cells. They are dispersed but also interconnected. The network will likely be amorphous and acephalous—it will have no precise heart or head, although not all nodes may be "created equal." As discussed below, the network may have a chain, star, or better yet, an all-channel design, though hybridization and multilayering are likely. For example, an all-channel network might send out a chain to fulfill some mission or to connect with an allied network. Colombian and Mexican drug gangs seem to interconnect in this fashion. Older criminal organizations, like the Mafia, appear to use star networks more frequently than all-channel formations, although linking via chains also occurs.

In addition to these structural elements, the netwar actor has behavioral dynamics that enhance both operational effectiveness and survivability. This type of actor has a great capacity for self-reorganization, allowing for adaptation to varied environments and challenges, and for the versatility needed to pursue a wide range of activi-

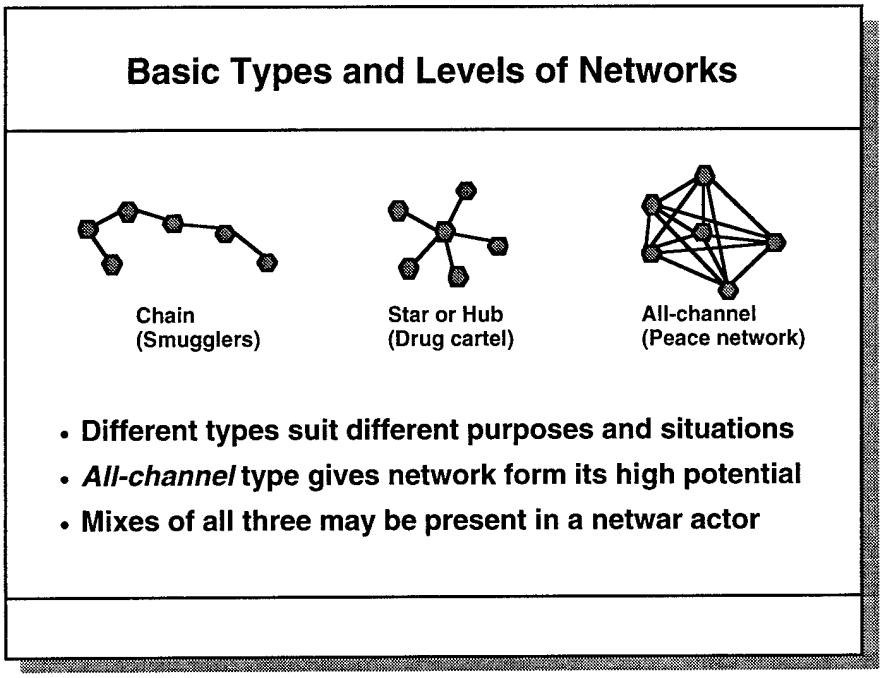
ties. These behavioral traits contribute to the robustness of the archetypal netwar actor when under attack, and also allow for smooth transitions from defense to offense. Indeed, the loose, somewhat dispersed attack formation of the network, discussed earlier, also serves as the principal alignment for defense.

Our basic proposition is that the more an actor uses network forms of organization, doctrine, strategy, and communications to engage in conflict or crime, the more it is a netwar actor. By implication, there are various types of netwar actors.

What specific forms will netwar take? Who may be the state and nonstate adversaries? What threats and challenges may they pose to U.S. interests, or to life in the international system? Preliminary answers are presented in this chapter. The variety of actors discussed include ethnic, nationalist, and separatist movements; criminal organizations; terrorists and other violent revolutionaries; cyberspace saboteurs; and militant social activist groups. This is not meant to provide a formal typology of the varieties of netwar actors, nor a detailed analysis of them, nor an analysis of literature about them—it is just a presentation that emerges readily from our inquiry into what is going on in the world.

As discussed below, a netwar actor's design, and its strength, may be analyzed at four levels: organizational, doctrinal, technological, and social. The discussion in this section often highlights one level or another in describing a particular type of netwar actor. But we do not attempt, at this stage of our research, to examine systematically each variety in terms of all four levels.

The cases examined in this chapter fall along a spectrum, ranging from conflicts that have substantial (though not predominantly) military components, to those that hardly look like war at all, in the traditional sense. As to actors, we focus principally upon nonstate groups and organizations, since these constitute the majority of current netwar actors. However, some states may transform themselves to wage netwar. Indeed, they may come to resemble, in essential ways, the networked nonstate actors that will likely constitute the typical "netwarriors" of the future. For the present, though, states involved in netwar tend to work through nonstate proxies (e.g., some Middle Eastern states' sponsorship of a wide variety of small groups that engage in terrorist activities).



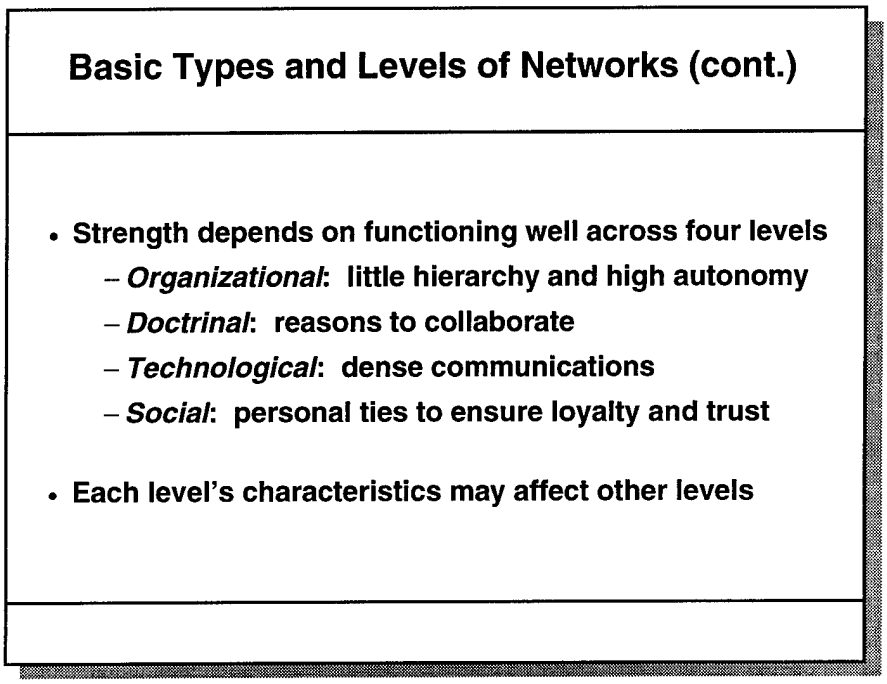

As the scholarly literature instructs, networks come in basically three types (or topologies):

- The *chain* network, as in a migration or job-search chain where people, goods, or information move along a line of contacts that are separated from each other, and where end-to-end communication must travel through the intermediate nodes.
- The *star*, hub, or wheel network, as in a franchise or a cartel structure where a set of actors are tied to a central (but not hierarchical) node or actor, and must go through that node to communicate and coordinate with each other.
- The *all-channel* network, as in a SPIN-like collaborative network of militant peace groups in which everyone is connected to everyone else.

Each node indicated in the diagrams may refer to an individual, a group, an institution, part of a group or institution, or even a nation-state. Each design is suited to different conditions and purposes. Of the three, the all-channel network is the most difficult to organize and sustain, partly because of the dense communications it may require. But it is also the type that gives the network form its new, high potential for collaborative undertakings. And it is the type that we generally refer to in this study.

All these types may be found among netwar-related adversaries, e.g., the chain among smuggling operations, the star among criminal syndicates, and the all-channel among militant groups that are highly internetted and decentralized. There may also be hybrids of the three types, with different tasks being organized around different types of networks. For example, a netwar actor may have an all-channel council or directorate at its core, but use stars and chains for tactical operations.

There may also be hybrids of network and hierarchical forms of organization. For example, traditional hierarchies may exist inside particular nodes in a network. Some actors may have a hierarchical organization overall but use network designs for tactical operations; other actors may have an all-channel network design overall but use hierarchical teams for tactical operations. Many different combinations and configurations are possible.




So far, we have not found an established academic methodology to follow for analyzing the networks that appear among netwar actors, although the literature identifies many factors and attributes to consider. What makes sense to us is to examine the design and operation (or form and function) of a network—be it a chain, star, all-channel, or hybrid— in terms of four levels of analysis:

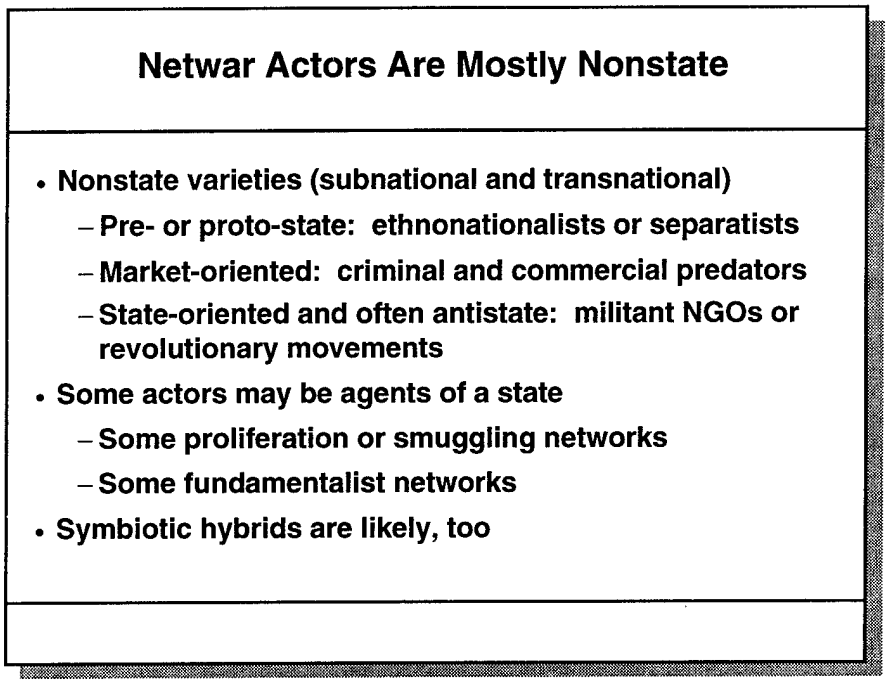
- *Organizational* level—To what extent is an actor, or set of actors, organized as a network? What type is it? This is the top level—really, the starting point—for assessing the extent to which an actor, or set of actors, is designed for netwar. Our earlier discussion of netwar design elements (see prior chart with that title) points out many considerations that should be taken into account. Among other things, assessment at this level may include inquiring whether and how members may act autonomously, but also whether and how hierarchical dynamics that preclude autonomy may be mixed in with the network dynamics.
- *Doctrinal* level—Why have the members assumed a network form? Is it deliberate? Fortuitous? What doctrines, ideologies, interests, and other reasons or motivations exist for their using and remaining in this form? This level of analysis is important for explaining what keeps a network together and enables the members to operate strategically and tactically without necessarily having a central command or leadership. The doctrine should reflect a commitment to collaborate and to remain in a network form (i.e., not change to a hierarchy). However, despite a generally shared world view, the network may include members who vary as to the priority of specific ends and the selection of means.
- *Technological* level—What is the pattern of, and the capacity for, dense information and communications flows? What technologies support this? How well do

they suit the organizational design? This level may involve a mix of new and old, high- and low-tech capabilities; but in general it is the new technologies that are making the new forms of organization and doctrine feasible. The higher the bandwidth, and the more advanced the means of transmission, reception, storage, and retrieval, the better the prospects for network-style communications and thus organization. Design elements and capabilities at this level may significantly affect the organizational and doctrinal levels.

- *Social* level—How well, and in what ways, are the members personally known and connected to each other? This is the classic level of social network analysis, where strong personal ties, often ones that rest on kinship, ethnicity, friendship, or bonding experiences, help ensure high degrees of personal trust and loyalty. To function well, networks seem to require higher degrees of interpersonal trust than do other forms of organization, like hierarchies. This traditional level remains important in the information age.

The strength of a network, perhaps especially of the all-channel design, depends on functioning well across all four levels. The strongest networks will be those in which the organizational level is supported by a pervasive doctrine or ideology attuned to the overall design and in which all this is layered atop advanced telecommunications and has traditional networks of personal and social ties at the base. Each level, and the overall design, may benefit from redundancy and diversity. Each level's characteristics are thus likely to affect the other levels.

In a well-developed network, the network itself may be considered more influential and important than any member (a dynamic that may help constrain any single member from dominating the network). The all-channel network may offer particular advantages in situations where the members aim to preserve their autonomy and independence and to avoid hierarchical controls, yet they also have agendas that are interdependent and benefit from coordination. Such a network may become most durable—it may even have a central coordinating office—when its members develop strategic, collective interests in being part of the network that may at times override their individual interests, and when they prefer to remain in this form rather than coalesce into a hierarchical institution as the network gains power and influence.




Most netwar actors who engage in offensive operations will be nonstate and/or stateless, at least in the near future. They will be sub- as well as transnational. However, as the low costs and risks and likely high gains from netwar are demonstrated, more and more states may realize the value of adopting this approach to conflict in the information age. Indeed, some netwarriors are already serving as agents of a state, as is a common practice in the Middle East.

Hybrids are likely to emerge. In some instances, states may sponsor, but not necessarily direct, nonstate netwar actors. In other instances, nonstate actors may sponsor states. These sorts of developments will enhance the effectiveness of both the networks and the states with which they link up, posing a formidable task for state actors waging defensive netwar.

One type of nonstate actor exists mainly within the nation-state, often as a subnational ethnic or separatist movement. Another type functions more in the interstices between states and includes transnational criminals and revolutionaries, and sometimes also militant NGOs whose activities erode nationalism. Of course, there are exceptions to this. For example, the Kurds, quintessential ethnic separatists, are located across the territories of several states. But these exceptions highlight a general rule that ethnonationalists and separatists operate within state boundaries, while criminals often operate across them. Both types, however, often harbor powerful, dangerous anti-state sentiments and aims.

A troubling aspect of the interplay between state and nonstate actors in netwar revolves around the possibility that, instead of the emergence of symbiotic relationships, nonstate actors may often oppose, or prey upon, states. In Colombia, transnational criminal networks, principally the drug cartels, have been hammering

away at state political, legal, and social institutions for decades, to the point at which the foundations of the state may be fatally undermined. Another case has arisen in the wake of the dissolution of the Soviet Union, where the Russian successor state finds itself besieged by powerful criminal networks that have, in many ways, come to drive and dominate the nascent market structures struggling to survive and empower the state.

Finally, we also see a third path for nonstate netwar actors: Instead of developing symbiotic relationships with states or intentionally preying upon them, networked organizations may use nation-states' territories as arenas for their competition with rival networks. The consequences for the states subjected to such activities will be conditioned by the course and outcome of the particular netwar in question. For example, Zambia has, for at least the past 20 years, been a principal battleground between transnational ivory poaching interests and the Wildlife Fund, which seeks to protect the dwindling African elephant population. The poachers have sought to "capture" various political, legal, and military institutions, while the conservationists have striven to foster local political reforms and to provide economic alternatives to the exploitation of elephants. Gibson's (1995) examination of this case points out that the poachers have undermined the state, while the conservationists have engaged, in many respects, in state-building. The outcome, as of this writing, remains uncertain, as the competing interests appear to be in equipoise.

In short, the current landscape of netwar is dominated by nonstate actors. However, their interactions with states are almost continuous, having effects that range from beneficial to pernicious. A key question revolves around the possibility that states might come to realize the strengths of networked forms of organization, and develop them for the explicit purpose of combating networked nonstate criminal, terrorist, or revolutionary organizations.

## Ethnic, Nationalist, Separatist (ENS) Conflicts Reflect Classic Social Level of Netwar

- **ENS conflicts often have ancient tribe-like (T) basis**
  - **Rest on kinship networks: families, clans**
  - **Have "chiefs" but resist formal institutions**
  - **Guided by pre-modern traditions, religions**
- **Clans oscillate between solidarity, segmentation**
  - **If not at war externally, often feud internally**
  - **Meanwhile, crime against outsiders is "legitimate"**
- **Recent cases have confounded U.S. policy, strategy**
  - **Somalis, Serbs, Chechens**
  - **U.S. "militias"**

During the Cold War, indigenous conflicts were often sublimated to the demands of the superpower rivals. Now, the international system seems to be returning to traditional polycentric, regionalized patterns of conflict. Thus ethnonationalism, religious revivalism, and separatism are fostering a resurgence of unruliness, with the principal actors generally operating at the sub- or transnational levels. Indeed, of the 35 wars ongoing in 1995, only 3 (in the Balkans, Kashmir, and the Western Sahara) featured major interstate elements. The rest are internal wars (Brassey's, 1995). In these, the combatants have mostly tribal organizational structures, onto which many appear to have grafted various aspects of information-age network designs. Because of this, these ethnic, nationalist, and separatist (ENS) conflicts represent an important variety of netwar, and a potentially fruitful study of netwar.

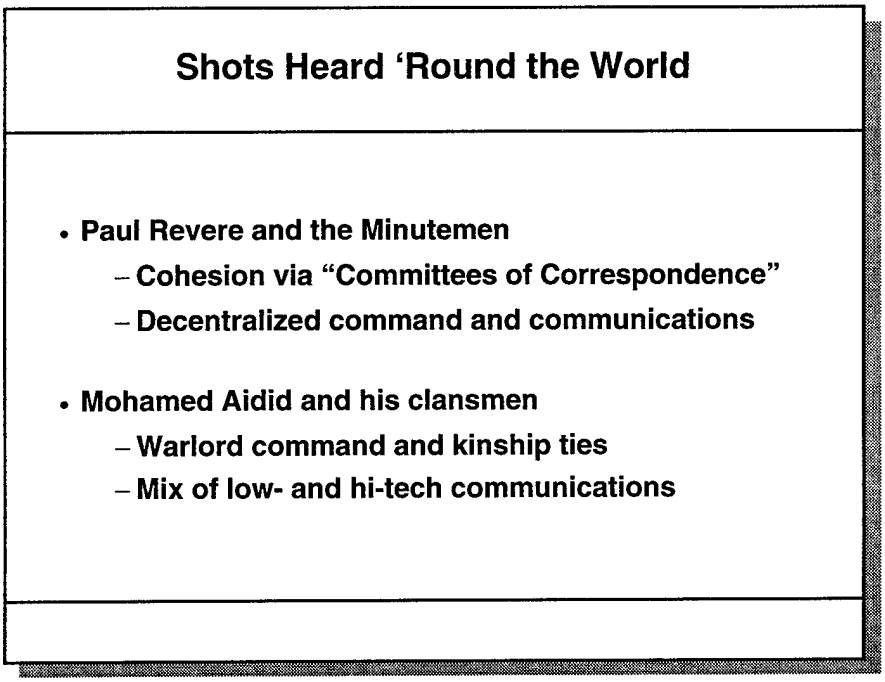
ENS protagonists are generally unlike nation-state actors. The former, and their organizations, are held together mainly by ethnic kinship ties. While many have a nominal "chief," there is, in reality, a dearth of formal, professional institutions; conduct is guided largely by premodern ethnic and religious traditions. Thus, we have the interesting phenomenon of netwar actors who graft N-type designs onto T-type structures, and who have little interest in building modern institutions and markets.

ENS organizations have proven well-suited to irregular warfare (and often to crime as well). Indeed, many exist in a state of almost perpetual conflict. When not fighting against a local government or outside power, their internal disputes often lead to internecine strife. (In anthropological terms, they oscillate between "fission" and "fission.") Thus, near-constant warfighting hones their skills and contributes to the development of ever more efficient network structures, making them formidable adversaries.

The recent American experience in Somalia exemplifies the difficulty of dealing with ENS adversaries; and at least one thoughtful study has focused on the need to understand the networked, organizational dimensions of the opponent in these sorts of conflicts (Allard, 1995). The long-standing resilience and intractability of the Serbs in the current Balkan War provide further evidence of the robustness of this kind of adversary, as the United Nations and NATO have learned that they must deal, beyond "chiefs" like Radovan Karadzic or Ratko Mladic, with countless clan members to whose demands the nominal leaders must be attentive, if not subservient. The current Russian trials in Chechnya reflect a similar struggle against a networked, clannish opponent that can withstand enormous damage and yet continue the fight. This case approaches the netwar ideal; the Chechen insurgents eschew traditional military structures in favor of cell-like "task groups" capable of an unusual degree of autonomous action.

Traditional warfighting approaches will continue to have little ability to defeat such adversaries. Those who wish to counter ENS opponents may have to adopt doctrines and organizational structures that resemble the insurgent networks they confront.

A recent example, still worthy of careful study even though it predates the current rash of ethnonationalist conflicts, involves the Viet Cong campaigns in the early years of the Vietnam War. Organized in cells and networks, these insurgents came close to toppling the regime in Saigon, which was propped up only by American intervention. U.S. forces, though quite effective militarily, employed an ill-suited "big unit" approach to fighting an opponent almost invulnerable to traditional military pressure (Summers, 1982; Krepinevich, 1992). The Viet Cong insurgency against the South Vietnamese and American forces highlights the robustness of the network when under attack by hierarchically oriented adversaries.




Consider the situation that the British colonists in North America faced in the mid-18th century, when the first major wars against the Indians flared. The immediate response of the British (and the settlers, including George Washington) was to send a traditional European-style field army off to the wilderness to pacify it. The result was the slaughter of General Braddock and his forces, followed by a newfound willingness to innovate. This led to much "irregularization" of colonial forces (Rogers' Rangers, etc.), and a great deal of tactical decentralization by the Crown commanders. In the end, this institutional redesign played as much a role in winning the French and Indian Wars as any of General Wolfe's heroics on the Plains of Abraham (Parkman, 1884).

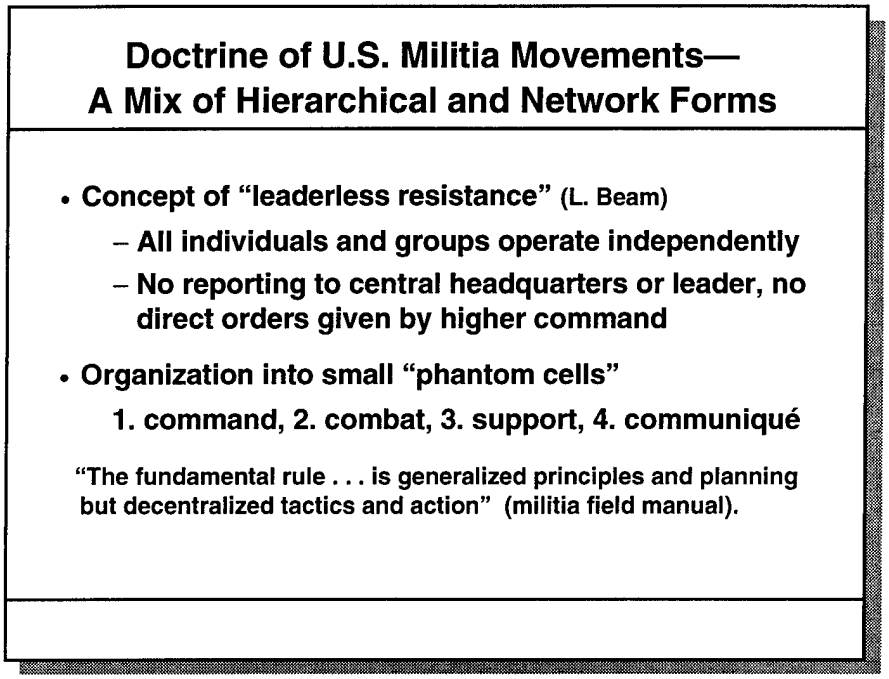
The irregular politico-military organizational structures that served the British colonists so well during the French and Indian War formed the basis of the militias that would start the fight for independence from Britain. Militia nodes soon covered the land, linked together, network-style, by the Committees of Correspondence. Although each cell was quite small, and most were geographically dispersed, strong communications links allowed for rapid mobilization and deployment. During the initial battles at Lexington and Concord, for example, this form of organization and its communications infrastructure allowed the rebels to engage in unrelenting "swarm" attacks against veteran British regulars, inflicting a costly, humiliating defeat on them.

After these opening battles, the rebels sped to write up their accounts of the skirmishes, dispatching them on the first available packet ship to Europe. They seized the initiative to win the information and propaganda war in Europe. The British, by engaging in procedurally proper after-action reporting—and being in little hurry to relay the debacle to military superiors, the Crown, and the British public—were thus

confronted with the fact that the rebels' view of the fighting had been circulating for weeks in Europe before official government reports became available (Fischer, 1994; Galvin, 1989).

Recently, Somali clan leader Mohammed Farrah Aidid used an internetted structure similar to that employed by the Minutemen, and mixed low- and high-technology instruments in his communications infrastructure. This gave him and his forces considerable defensive robustness and allowed them to monitor the movements of U.S. Rangers sufficiently closely to permit a shift to the tactical offensive that helped unravel U.S. policy. Indeed, the swarming tactics used by the Somalis during their long firefight with Task Force Ranger are reminiscent of the command and control of the Minutemen in the battles of Lexington and Concord.

Further, it must be observed that Aidid was extremely aware of the importance of directing the flow of information about this action away from the fact that his fighters suffered grievous losses. Instead, he successfully kept the focus on the issue of U.S. casualties, which directly affected the resolve of the American public and political leadership in sustaining its campaign against him.




Clannish structures dominated by ethnic concerns appear among some contemporary white supremacist groups in the United States. A doctrine of "leaderless resistance" elaborated by one extremist leader, Louis Beam, shows—disturbingly, but with great relevance for understanding netwar in the information age—the importance of doctrine for organization and behavior. This particular doctrine downplays hierarchy in favor of a network of "phantom cells." It reveals a belief that the more an extreme right-wing movement conforms to networked organizational designs, the more robust it will be defensively, and the more flexible offensively.

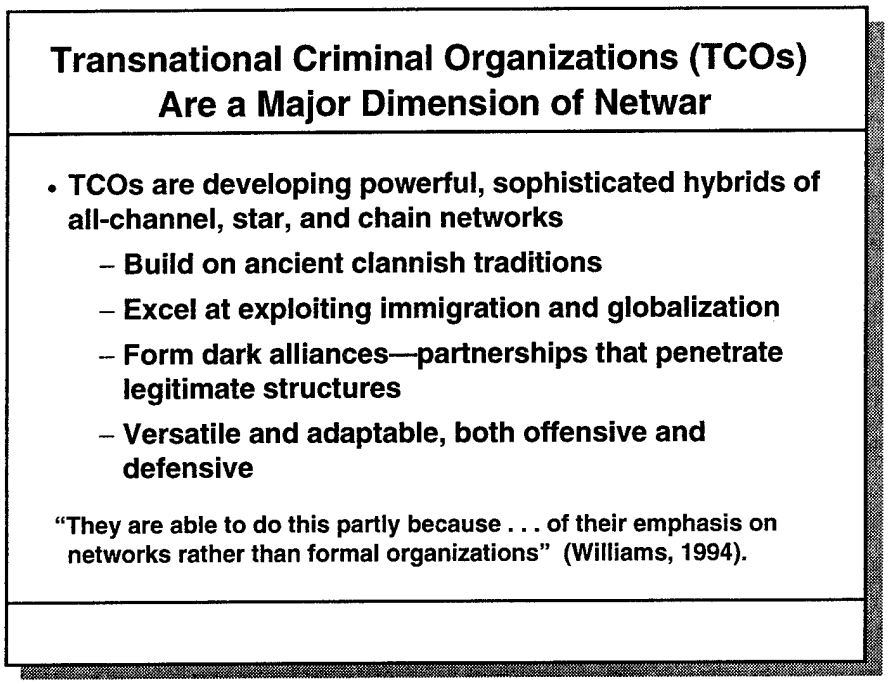
> Utilizing the Leaderless Resistance concept, all individuals and groups operate independently of each other, and never report to a central headquarters or single leader for direction or instruction . . . participants in a program of Leaderless Resistance through Phantom Cell or individual action must know exactly what they are doing, and exactly how to do it.
>
> Since the entire purpose of Leaderless Resistance is to defeat state tyranny . . . all members of phantom cells or individuals will tend to react to objective events in the same way through usual tactics of resistance. Organs of information distribution such as newspapers, leaflets, computers, etc., which are widely available to all, keep each person informed of events, allowing for a planned response that will take many variations. No one need issue an order to anyone (Beam, 1992).

Beam's doctrine calls for four types of cells: (1) command, (2) combat, (3) support, and (4) communiqué. Each cell consists of about eight "minutemen" and has its own leader. This allows for a specialization of function and tight security precautions.

Similar doctrinal instructions reportedly appear in a manual used by U.S. militias that, while not necessarily white supremacist, have objectives and worry about threats that call for a secretive, decentralized cell structure:

> The fundamental rule guiding the organization of the free militia is generalized principles and planning but decentralized tactics and action.
>
> What is meant by this key statement is that the whole militia must be committed to the same cause and coordinated in their joint defense of a community. Thus, there must be allegiance to a higher command. But specific tactics should be left up to the individual elements so that compromise of a part does not compromise the whole. Furthermore, all training and combat actions should be up to the smaller elements, again so that isolation or decapitation does not render the smaller units inept.
>
> The way a balance between these competing concerns is achieved in the free militia is to organize all elements into "cells" (*Field Manual Section 1: Principles Justifying the Arming and Organizing of a Militia*, Wisconsin: The Free Militia, 1994, p. 78).

These are important tenets for netwar; they show the importance of the doctrinal level for analyzing netwar actors and are consistent with the concept of SPINs mentioned earlier. Although the quotations are drawn from writings about U.S. right-wing groups, they hark back to the U.S. Committees of Correspondence, and to European anarchist doctrines. Overall, they reflect a looser approach to decision-making and operations than traditionally found in right- and left-wing movements—compare, for example, to Mao Zedong's doctrine that "command must be centralized for strategic purposes and decentralized for tactical purposes." (See Burghardt, 1995a, and 1995b, from which the quotations are taken; and Stern, 1996.)




Transnational criminal organizations (TCOs), though eminently modern, have a long history, dating at least from the pirate networks that ravaged Mediterranean trade during the first Caesar's day. The Muslim Cult of the Assassins was organized similarly, operating over a wide territorial base. Finally, the Italian Mafia, the Chinese Tongs, and the Japanese Yakuza have clear roots in the Middle Ages.

The ability of TCOs to prosper in international systems dominated first by empires and later by states lies in their tight kinship ties and loosely knit networked structures. That they have long practice in coping with hostile environments implies their likely continued success in an increasingly interconnected world in which the dominant political entities (states) are growing ever more "soft-edged."

TCOs, as Phil Williams has pointed out, are a burgeoning problem in the information age, in large part because they are extremely well-suited, organizationally, to operate in an era marked by greater interconnectivity:

> TCOs are diverse in structure, outlook and membership. What they have in common is that they are highly mobile and adaptable and are able to operate across national borders with great ease. They are able to do this partly because of the conditions identified above and partly because of their emphasis on networks rather than formal organizations (Williams, 1994, p. 105).

TCOs are developing sophisticated hybrids of all-channel, star, and chain networks that build on long traditions of clannish networking. They excel at exploiting trends that enhance interconnectivity. They are versatile and adaptable and have a proclivity to form odd alliances and partnerships that can penetrate legitimate political structures.

TCOs have developed alarming offensive as well as defensive capabilities. Criminal predations in Colombia provide a clear example of the creation of a virtual "kleptocracy," where legitimate institutions must continually fight for their autonomy. This war is waged by criminal networks in loose alliances (cartels) that draw resources from their international operations. Colombia has little ability, alone, to combat transnationalized opponents. Even the recent captures of cartel leaders have had only modest effects, because the cartels are organized in mixed all-channel, chain, and star networks, which are not easily susceptible to counterleadership targeting.

The threat of states besieged by TCOs is not unique to Colombia. Russia faces a similarly stern challenge from a variety of criminal enterprises, of which the Chechen Mafia is only one. Italy has recently learned of sophisticated penetrations of its institutions by the Sicilian and American mafias (e.g., the indictment of former Prime Minister Giulio Andreotti for colluding with the Mafia). Perhaps more troubling is evidence that, as states often form alliances, TCOs are entering into dark pacts, carving out spheres of influence and making common cause wherever possible, as the late Claire Sterling noted (1994). States, loath to cede any sovereignty, have great difficulty coping with such enterprises, though the recent establishment of Europol shows some willingness to relax sovereignty in return for enhanced crime-fighting capabilities.

Criminals often use methods of "epistemological warfare" as they insert themselves deeply into the fabric of societies, embrace nationalism, act like "Robin Hoods," and corrupt their governments' foreign and domestic policies. Examples abound in Colombia, Italy, Mexico, and Russia.

Some states use criminals to pursue national goals. China sponsors both intellectual and maritime piracy. The former invigorates the economy, its competitiveness, and trade balance. Sea piracy (e.g., of oil tankers) abets Chinese efforts to exert hegemony over the Spratly Islands. Harassment by pirates presumably makes other governments succumb to Chinese claims that its presence is needed to control the threat. The example of the East Asian pirates is not unlike the curious relationship of the Royal Navy and the Barbary Pirates in the early 19th century. Britain fostered their depredations against ships of other, competing nations (including the United States). This drove much international trade onto British flag vessels and had profound effects on the costs of goods in many countries.

## Deep Roots and Long Branches of TCOs

- **Criminal netwar is a burgeoning, global problem**
  - **Proliferation, smuggling, theft, manufacturing, and money laundering**
  - **China, Colombia, Italy, Japan, Mexico, Nigeria, and Russia**
- **Difficult to combat**
  - **TCOs are becoming the basis or agent of state power in some instances—the "shadow state"**
  - **Interagency cooperation within and across borders is increasingly required to combat TCOs**

Criminal netwar appears in the arms and drug trades, trafficking in illegal immigrants and merchandise, and money laundering. States with acute TCO problems include China, Colombia, Italy, Japan, Mexico, Nigeria, and Russia. In the post–Cold War era, TCOs benefit from the unsettled nature of the international system and from the strains that so many states are suffering. Uncertainty about alliances and about security guaranties fosters a thriving demand for arms, including weapons of mass destruction, and TCOs have tried to fill the role of supplier. Increasingly, competitive economic relations put a premium on intellectual property, another area into which TCOs have moved. Economic dislocation and internal conflict have induced masses of people to emigrate by any means, providing yet another opportunity for illicit activity. The drug trade remains a key activity, though these other "profit centers" suggest that TCOs, like successful corporate ventures, can diversify into many areas in which they have comparative advantages.

While TCOs often sought to coexist with states in the past, their new activities have increasingly corrosive effects on state power, signaling the possibility of serious clashes with states (Anderson, 1989; Clutterbuck, 1990). This implies two plausible TCO strategies. First, the TCO might choose to cooperate with one or a few state "hosts," becoming an unusual basis and agent of state power. The other strategy would pursue a more confrontational approach, fending off state control, or, in some instances, establishing an informal "shadow state" to co-opt the host.

Our look at TCO operations and interactions suggests that both strategies have enjoyed substantial success. In terms of collaboration with a host state, China stands out as a preeminent example. Despite official calls for an end to corrupt practices and ties to organized crime, there is abundant evidence of a substantial symbiosis, particularly in areas relating to illegal immigration and to industrial espionage

(Bresler, 1981). The Chinese diaspora offers fertile ground for the establishment of ties to Chinese TCOs, suggesting that, as concern grows about China's emerging great-power status, there should also be a growing awareness of its tremendous potential for netwar, not least in terms of its use of TCOs.

Another, albeit lesser, case is the collaboration of the Nigerian government with various TCOs. As in China's case, the Nigerian state is not imperiled but has a principal-agent relationship with the TCOs. Similar issues may also be raised about Mexico, where drug traffickers have built a full range of operations. But in this case, the available evidence suggests that the TCOs may be trying to "capture" parts of the Mexican government. Russia appears to have a similarly fractious relationship with the many TCOs plying their trades on Russian territory, and the Japanese Yakuza can be seen as engaging in similar efforts, though in this case their targets are industrial concerns (Vaksberg, 1992; Kaplan and Dubro, 1986).

In two cases, TCOs have mounted sustained assaults on the foundations of statehood: in Colombia and Italy. In the former case, these activities have come perilously close to causing the "failure" of the state itself. In the Italian case, Mafia predations have helped to divide Italy between the increasingly impoverished South, where organized crime's power is greatest, and the prosperous North, which has thus far been reasonably well-defended.

As these cases indicate, TCOs have a great strategic and tactical flexibility that results partly from their networked natures. Thus far, governments have had mixed results dealing with them. Part of the problem is that hierarchical institutions are often ill-suited to grapple with networked opponents. To adapt, governments have begun to adopt internal reforms, so that "stove-piped" bureaucratic approaches to law enforcement give way to interagency (i.e., network-like) approaches. Governments may also have to be willing, externally, to relax sovereignty enough to foster the rise of transnational crime-fighting mechanisms that are capable of the same nimbleness of maneuver across borders as exhibited by the TCOs. The next chart provides an example of just this sort of development.

## Southeast Asian Piracy: Instructive Case of Criminal Netwar and Counternetwar

- Resurgence is serious (echoes of 19th century)
  - Pirates developed multinodal structures
  - Attacks posed financial and environmental risks
- State-by-state responses failed
  - Joint efforts inhibited
  - Pirates circumvented countermeasures
- Network-style innovations are working
  - Intermilitary information sharing
  - Relaxation of state sovereignty

The recent resurgence of piracy in Southeast Asia[1] provides a valuable case for examining netwar and counternetwar strategies and operations. This resurgence, which echoes the activities of the Penang and other Southeast Asian pirates of the 19th century, has posed serious financial and environmental risks. In addition to the values of commercial ships and their cargoes in general, the pirates have focused on attacking oil tankers. Sometimes, fearing interception, the pirates have abandoned their raids, leaving tanker crews bound and gagged while their ships run without piloting, sometimes for hours, in the narrow Strait of Malacca. Back in the 19th century, the Royal Navy faced few political or legal constraints and could deal summarily with such pirates. Today, these waters are divided among a number of states, all of whose sovereignty claims must be respected. The pirates, who have developed multinodal structures and sometimes engage in loose principal-agent relations with regional states, have taken full advantage of their balky, hierarchical adversaries.

Initially, those states whose territorial waters were the scenes of piracy (Indonesia, Malaysia, Singapore, and the Philippines) attempted to resolve the problem independently of each other. These efforts failed miserably during the late 1980s and early 1990s, because the pirates learned to move in and out of territorial waters, much as American gangsters of the 1920s and 1930s were able to avoid local and state police by crossing state lines.

With incidents of piracy rising at a precipitous rate (about 20 percent per year), local states decided to share additional intelligence and went so far as to engage in cooperative interdiction efforts. More-decentralized command and control systems

[1] Facts and figures used herein derive from the *Violence at Sea Database* (1995).

emerged, allowing for rapid responses. Even some relaxation of state sovereignty occurred. Military and police elements, within and between these countries, began to coordinate more directly and continuously. Within a year, piratical incidents in Southeast Asia fell by 50 percent. In 1994, no acts of piracy occurred in the Strait of Malacca. The networked response to dealing with the pirates was working, in the wake of the failure of traditional state-by-state responses to the problem.

This is a fine example of network-style innovations working to combat an age-old problem that once again threatened the freedom of the seas. Success came through both intermilitary (and police) information sharing and the relaxation of state sovereignty. Interestingly, the pirates appear to have picked up their operations and moved them to the vicinity of the Spratly Islands, an area riven by conflicting sovereignty claims. There is some evidence, though it is not conclusive, that China is tolerating these pirates. In any case, the 40 percent increase in pirate attacks in this area suggests that, where international and interorganizational cooperation are lacking, such depredations may flourish.

Finally, it is crucial to note that these pirates, though tied into a tradition as old as history, have shown great interest in and sensitivity to the tools and organizational concepts of the information age. Thus, they frequently locate buyers for their contraband (including oil) on the "spot market," and sometimes create new identities for seized ships and their cargoes. These "phantom ships," which are real, are occasionally used as the basis for creating fictitious doubles, which are then insured, "lost at sea," and submitted to claims for insurance reimbursement. Surely, the Cilician pirates from Roman days, or the Barbary corsairs, would nod in proud wonder at such activities. To cope with pirate networks that support the phantom ship business, a whole new set of intelligence and operational skills will be needed.

## Revolutionary, Terrorist Organizations Are Reforming into Networks

- **Long history but new trend of subversive networking to offset state power**
  - **Recent movement away from Leninist hierarchies, toward semi-autonomous cellular structures**
  - **Pushed in this direction by U.S. preponderance?**
- **Reminiscent of "SPINs" (segmented, polycephalous, integrated networks)**
- **Examples: Hamas and Hezbollah—contrast to PLO**

Revolutionary and terrorist groups have been players in world politics since at least the days of the Zealots, who tried to free Palestine from Roman rule two thousand years ago. Lewis Gann's (1971) rich history of these groups documents that they have had a common tendency toward centralized leadership and hierarchical control. In the 20th century, Leninist views about the importance of centralized control, no doubt growing out of the centralized Bolsheviks' success in 1917 Russia, have culminated in the *foco* theory of guerrilla warfare expounded by Fidel Castro and Ernesto "Che" Guevara (Goren, 1984). However, centralized leadership, which worked well in a militarily defeated, war-weary Russia, may, under most other conditions, make revolutionary and terrorist organizations vulnerable to counterleadership targeting, a tactic often used against them, and one that continues to cripple those that maintain hierarchical structures. Thus, *Sendero Luminoso* in Peru suffered severely when its charismatic leader, Abimael Guzmán, was captured, and the Islamic Brotherhood was put virtually out of business when its commander was assassinated in late 1995 in Malta.

Now, perhaps partly in response to the increasing vulnerability if not obsolescence of Leninist and Fidelista designs in a world defined by U.S. preponderance, many revolutionary and terrorist organizations are adopting networked command structures that are segmented and polycephalous (i.e., having a number of commanders who are positioned at various nodes but who are able to exert strategic control over the whole network). This new approach to their organization harks back to the SPIN design (see p. 10 above) that is increasingly found among netwar actors.

Historically, efforts to counter terrorists and revolutionaries have centered either on the establishment of preclusive security procedures to protect vulnerable places and people, or on the infiltration of these radical groups. Preclusive security has never

resulted in "leak-proof" point defenses, as even the most vigorous programs (e.g., Israel's) indicate. Infiltration has also had a problematic record, because the terrorists' networks limit the damage that an infiltrator can inflict prior to exposure. Moreover, many years may be required to move into a position of authority, with advancement contingent upon the commission of acts of terrorism. Thus, in addition to the matter of temporal constraint, the infiltration option runs up against Western normative inhibitions about committing terrorist acts as part of combating terrorism (see Rivers, 1986).

The evolution of terrorism (and criminal organizations, militias, etc.) has been from cells arranged and controlled hierarchically (Laquer, 1979) to networks of cells, with a new mix of civilian and military elements. For example, the PLO has highly centralized decisionmaking around a common doctrine and dominant leader (Yasir Arafat). In contrast, Hamas has devolved much decisionmaking authority to local cells, eschewing a "cult of the leader" (Cobban, 1984).

Aum Shinrikyo, the Japanese religious cult responsible for the recent series of chemical attacks throughout Japan, may provide an example of a new, hybrid type of organization. It is hierarchical, in the sense that the leader (now under arrest) embodied the doctrine of the cult, providing its overarching sense of vision and mission. Operationally and tactically, however, the organization appears to have been quite decentralized. Nevertheless, because of the centralization of its strategic and doctrinal dimensions, the cult was still susceptible to serious damage as a result of the loss of its leader. Thus, a key implication for counternetwar may be to continue to focus operations against any remaining hierarchical elements in the terrorist or revolutionary organization's institutional design.

Finally, the dilemmas posed by these changes in terrorist organizations imply that governments might be well advised to adopt an information-based counternetwar to combat terrorism. When protecting persons or places or infiltrating terrorist groups seems problematic, then detecting, monitoring, tracking, and anticipating terrorist moves, particularly those of semi-autonomous cells, will prove of paramount importance. This issue is discussed further in the doctrine and strategy portion of this study.

## Cyberspace Terrorism and "Cybotage": A Growing Concern

- **Information warfare will increasingly attract anarchists, nihilists, "cyboteurs," spies, and terrorists**
  - **Some will operate as loners, others in leagues**
  - **Many, but not all, will qualify as netwar actors**
- **Motivations will vary from societal to personal**
  - **Ideational (e.g., retribution against power)**
  - **Mercenary or self-exalting**
- **Disrupt-and-destroy potential alarming . . . but how?**
- **Significance depends on links to other types of netwar**

Cyberspace is an increasingly attractive venue for terrorism and sabotage. The list of actors who may be drawn to cyber-terror or "cybotage" is long and includes anarchists, nihilists, and anarcho-syndicalists, at one end of a spectrum, and societal misfits, disaffected scientists, disgruntled employees (or ex-employees) and hackers at the other. Many such actors today operate primarily as loners (e.g., Kevin Mitnick) or in juvenile leagues (e.g., the Legion of Doom). This will likely remain the case to some extent, perhaps because this phenomenon is still in a formative stage (Hafner and Markoff, 1991). But meanwhile, more sophisticated, better organized actors are emerging, including "cyber mercenaries" and information warfare specialists who may be developed from within or recruited into the ranks of terrorist or revolutionary organizations or cults (e.g., the Church of Scientology has apparently recruited or developed a cadre of netwarriors to deal with dissidents and apostates).

Cyberspace offers opportunities for such actors to inflict costly, disruptive damage, but without inflicting the physical and human destruction that so often arouses the ire of victims, or that may even alienate the affections of the terrorists' sponsors or constituencies. Unlike blowing up planes or killing hostages, disrupting the flow of information can inflict enough pain to convey the symbolic message so central to terrorism, while avoiding the more unsavory aspects of traditional destructive terrorism.

A reason for terrorists to move into cyberspace is to cause disruptions that have widely diffuse effects. Previously, terrorist attacks tended to cause serious physical damage in limited spaces (though the repercussions through the media may have been global). The easing of spatial limitations on the direct effects of acts of terror should prove quite attractive. Finally, terrorists will find, no doubt, fertile ground for recruits willing to engage in acts of "cybotage."

Of course, one cannot overlook the possibility that terrorists themselves will see merit in becoming as adept at computer hacking as they try to be at killing (Reich, 1990). An ability to threaten the national information infrastructure (NII) and C3I systems gives terrorists another way to command media attention, thereby affecting the primary means by which Americans inform themselves about the world. Such a prospect poses the opportunity to make great gains, while controlling risks and doing little violence to innocent people. Indeed, for some terrorists, netwar may provide the best of all worlds.

Compared with other types of netwar, this type is one of the easiest about which to be alarmist at this stage in the information revolution—but it is also the type whose implications for netwar are among the most uncertain. It is relatively easy to concoct havoc-wreaking scenarios (Collins and Lapierre, 1979; Hundley and Anderson, 1996; Kupperman and Kamen, 1989; Schwartau, 1994). Yet, it is unclear whether these scenarios are realistic. This is reminiscent of extreme terrorism scenarios of the 1970s and 1980s, in which the United States may be momentarily brought to its knees—but, so far, such scenarios have not unfolded, in part because they presume both ends and means that, in fact, lie beyond the reach of terrorists and should continue to do so as defenses form and spread.

Often when we have presented the concept of netwar, audiences have presumed the term denotes primarily the types of actors discussed on this chart: cyberterrorists, cyboteurs, and various societal misfits who have the skills of hackers. While these actors sometimes fit the pattern of netwar, this is not always the case. It is particularly not the case for the lone hacker who is simply engaging in vandalism in cyberspace. It is more the case where such actors have links to, or are members of, an organized network that has clear goals and missions, and cohesive doctrines for effecting them. Indeed, the significance of cyberterrorists and cyboteurs for netwar may depend upon their "fit" into the other types of actors discussed here (e.g., those having to do with ethnonationalist struggles, criminal enterprises, or militant civil-society conflicts). Lone hacker Kevin Mitnick is far less a netwarrior than the Zapatistas' Subcomandante Marcos.

## Transnational NGO Activism: The Vanguard of Social Netwar

- **Transnational network structure being built up**
  - **Emphasis on "collective diversity" and "coordinated anarchy"—no central leader, ideology, or issue**
  - **Communications systems for consultation and mobilization**
- **Doctrine and strategy**
  - **Make civil society the vanguard—construct "global civil society" and connect to local NGOs**
  - **Make "information" the decisive weapon—demand free flows of information, capture media attention**
- **A challenge but not necessarily a threat to U.S. interests**

Social struggles form another arena where netwar is on the rise. Since the 1970s, the world has entered an era of "new social movements"—of information-age activism based on associations among NGOs concerned with modern and postmodern issues such as the environment, human rights, immigration, indigenous peoples, cyberspace, etc.[2] When such struggles turn militant, there is usually evidence of "social netwar."

We see this, for example, in the domestic U.S. conflicts about abortion and environmental issues (e.g., see Chase, 1995), and at the global level in the campaigns of human-rights organizations against dictatorial regimes. Elements of social netwar appear in efforts by Chinese students abroad to aid their companions in Tiananmen Square, in alliances among American and European "skinhead" groups, and in the global campaign by Greenpeace and its allies to try to compel the French government to halt nuclear testing in the Pacific. While these particular examples do not represent clear victories by nonstate against state actors, they help define a trend and indicate that governments are going to need great agility and adaptability to cope with threats and challenges from social netwarriors in the coming decades. Yet, it is far from clear that NGOs will be able, as a rule, to erode state power.

Our comments focus on the rise of netwar-related forms of organization, doctrine, strategy, and communications to support transnational activism. Social netwar at this level is conducted largely through vigilant swarming. And to this end, a global

[2]Bibliography on this phenomenon is still sparse. Sources, in addition to those cited earlier regarding the rise of civil society, include Boulding (1988); Brecher, Childs, and Cutler (1993); such academic volumes on "new social movements" as Laraña, Johnston, and Gusfield (1994), and Morris and McClurg (1992); and a special issue of *Social Research*, Vol. 52, No. 4 (Winter 1985).

network structure is being built up. It consists of issue-oriented groups (such as Doctors Without Borders) and infrastructure-building organizations (such as Global Exchange) that can mount a campaign around any issue. This structure has no central leadership or ideology, although some activists and political tendencies may be stronger than others. Instead, it is characterized by what we call "collective diversity" and "coordinated anarchy"—once a focus arises (e.g., Mexico), activist NGOs that find any connection to their specialty (e.g., peace, sustainable development, etc.) may join the swarm and choose autonomously but consultatively in which actions to participate. Building a communications infrastructure (like the APC networks—see pp. 23–24) that enables rapid mobilization is very important to this structure.

Doctrine and strategy for transnational social netwar remain nascent, but some outlines have emerged. Briefly, as we have noted elsewhere, they involve making civil society the vanguard—and constructing a "global civil society" that can connect to local NGOs, and that can counter state and market actors. They also include "information" as the decisive weapon. Indeed, in a social netwar in which a set of NGO activists challenge a government or another set of activists over a hot public issue, the battle is largely about "information"—about who knows what, when, and where. A social netwar involves seeking total intelligence or "topsight" (Gelernter, 1991) about one's own and the opponent's situation, while keeping that opponent in the dark about oneself and, if possible, about its own situation. It involves affecting what an opponent knows, or thinks it knows, not only about its challenger but also about itself and the world around it. Among other things, this may mean trying to shape images, beliefs, and attitudes in the social milieu in which both are operating. A social netwar is thus likely to bring demands for freedom of information and battles for public opinion and media access and coverage to local and global levels. It may include propaganda and psychological warfare, not only to inform but also to disinform. It may well resemble a nonmilitary version of Szafranski's (1994, 1995) notion of "neo-cortical warfare."

Many varieties of netwar—e.g., criminal and terrorist—that we discuss in this document threaten U.S. interests. We do not mean to imply that *social netwar* also generally poses a threat. Indeed, as noted below, social netwar may sometimes benefit U.S. interests. Our point is that transnational NGO activists are on the cutting edge of developing new network forms of organization, doctrine, and strategy—and whoever wants to understand netwar dynamics would be well advised to study their innovative models.

## Mexico Provides Major Example of Transnational Social Netwar

- **Subnational and transnational actors link to confront state lagging at democratization and development**
  - **Zapatistas nearly trigger counterinsurgency**
  - **Influx of transnational activist NGOs restrains government and alters context of struggle**
- **New model of conflict tested by "netwarriors"**

**"Chiapas . . . is a place where there has not been a shot fired in the last 15 months. The shots lasted 10 days, and ever since the war has been a war of ink, of written word, a war on the Internet"**

**— Mexico's Foreign Minister Jose Angel Gurria, April 1995**

- **Mixed results (counternetwar also under way)**

In Mexico, a mix of subnational and transnational actors have mounted a social netwar against a state lagging at democratization. The netwar appears in the decentralized collaboration among the numerous, diverse Mexican and transnational (mostly U.S. and Canadian) activists who side with the Zapatista National Liberation Army (EZLN), and who aim to affect government policies on human rights, democracy, and other major reform issues. Mexico, which generated the first successful social revolution of the 20th century, is now the scene of a prototype for social netwar in the 21st century.

The Zapatistas are insurgents—in some eyes, the first post-Communist, postmodern insurgents. But the dynamics that make their insurgency so different—notably, the strategic links to activist NGOs—move them out of an "insurgency" into a "netwar" framework. Without the influx of foreign NGO activists, which began hours after the EZLN's insurrection on New Year's Day 1994, the dynamics in Chiapas might have deteriorated into a conventional insurgency and counterinsurgency—and the small, poorly equipped EZLN might not have done well. Transnational NGO activism, not the novel insurgency per se, is what changed the framework.

The EZLN's artful "Subcomandante Marcos" says that a new model of social conflict and transformation is being tested. He and his cohorts have eschewed Leninist, Maoist, and Fidelista models that call for an army or a party to seize power as the vanguard of revolution. Instead, their agenda (e.g., political democracy and regional autonomy) is more reformist than revolutionary (Castañeda, 1995). They deny that they want state power (though they aim to change the state). According to Marcos, "It is civil society that must transform Mexico—we are only a small part of that civil society, the armed part. . . ." The activation of civil society—not the expansion of an insurgent army—is the key feature of their doctrine.

NGO activists—some call themselves "netwarriors"—realize that they are developing a new model of conflict (e.g., Cleaver, 1994). For many, nonviolent but compelling action is crucial; and to this end, they need rapid, far-reaching communications, and freedom of information and travel. Much of their netwar has been waged in the media—in both old media like newspapers, magazines, and television, and new media like faxes, e-mail and computer billboard and conferencing systems. Since word of the insurrection first spread, the activists have made heavy use of the Internet (and systems like Peacenet) to disseminate news, mobilize support, and coordinate actions. Each side has waged public-relations battles to affect public perceptions of the other. Thus, in April 1995, Foreign Minister Jose Angel Gurria could comment that

> Chiapas . . . is a place where there has not been a shot fired in the last fifteen months. . . . The shots lasted ten days, and ever since the war has been a war of ink, of written word, a war on the Internet.

This social netwar has been partially effective. It helped compel President Carlos Salinas in January 1994, and President Ernesto Zedillo in February 1995, to halt army operations and turn to political negotiations in Chiapas. It has added to the national pressures on Mexico's rulers to enact political reforms, take human rights more seriously, accept the rise of civil society, and heed the needs of indigenous peoples. It may also be obliging the Mexican army to adopt institutional changes. In such respects, this netwar has not been bad for Mexico (or for some U.S. interests), even though it has heightened uncertainty about Mexico's stability.

This netwar, and the government's efforts at counternetwar, are far from over. Although the EZLN amounts to a figurative "army-in-being" that poses more a symbolic than a real threat of violence, the Zapatistas and their civil-society allies have effectively challenged and disrupted the Mexican system. The high visibility of the episodic peace negotiations in Chiapas, the unusual national poll known as the National Consultation, and the mixed results of the National Democratic Conventions sponsored by the EZLN attest to this. More to the point, the netwarriors evidently have a capacity to keep up the pressure, as just indicated by the creation of a nonmilitary FZLN (Zapatista National Liberation Front), whose aims include rallying nationwide support among marginalized indigenous peoples, and pressing for reforms independently of political parties.

## Implications Extend Far Beyond Mexico

- **Conditions for social netwar to be effective**
  - **Society should be partly open, under strain, and have local counterparts for transnational NGOs**
  - **Society should be in region where activists have transnational communications infrastructure**
- **Netwar may prove potent for affecting some nations**
  - **Disrupting authoritarian regimes**
  - **Spurring democratic reforms**
- **Future cases:**
  - **Cuba, Nigeria, Russia, or Saudi Arabia?**
  - **New global peace and disarmament movement?**

This Mexican prototype has implications that extend beyond Mexico, for it indicates conditions that should be present for a transnational social netwar to develop. As in the case of Mexico, a society should be relatively open (or opening up), particularly as regards freedom of information. It should be in flux and under political, economic, and other strains that are generating public debate; this may be the case especially where traditional clannish and hierarchical structures are challenged by, and adapting with difficulty to, new market and civil-society forces. The society should also have local NGOs that transnational NGOs can link to—more to the point, the society should be in a region where the transnational infrastructure for social activism is growing in both organizational and technological terms.

Because such conditions are not present everywhere—e.g., they apply far less to Myanmar than to Mexico—social netwar may affect some nations more than others. Where the conditions are ripe, the Mexican case implies that social netwar may work to disrupt authoritarian regimes and compel them to make democratic changes. Social netwar is in its infancy as a mode of conflict, and governments are just beginning to learn about it, but its importance and effectiveness are likely to grow around the world.

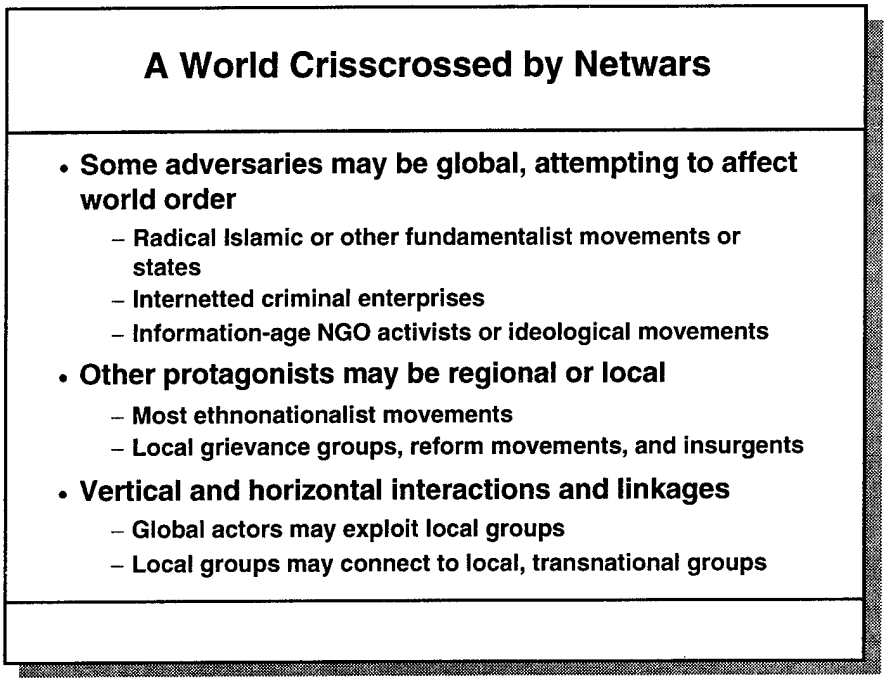
The scenes of future social netwars could include such countries as Cuba, Nigeria, Russia, and Saudi Arabia, to mention a few possibilities. In Cuba, the prospects for social netwar are increasing. Castro's government has begun to open up the economy but persists in political and social repression. Meanwhile, grassroots groups are trying to open space for activities within Cuba and gain connections to outside NGOs, including through faxes and e-mail (Gonzalez and Ronfeldt, 1994). Aspects of netwar have been present for decades in U.S.-Cuban relations, notably in the U.S. broadcasting and Cuban jamming of Radio Martí, as well as in the activities of pro-

and anti-Castro groups in the United States. What may be emerging now are the conditions for a full-fledged social netwar.

In Saudi Arabia, the ruling family retains tight control of the country, including through heavy surveillance and security measures. But an underground exists, and people's access to modern telecommunications is improving as a result of new connections to the Internet and plans for AT&T to upgrade the cellular telephone grid. Thus, the opportunities may improve for an indigenous dissident movement to develop that has links to outside fundamentalist and even secular democratic forces. At the same time, the more Saudi Arabia's telecommunications systems become connected to the outside world's, the higher the costs of repression and control will become for the ruling regime. Note, for example, that even a deliberately information-age autocracy like Singapore's cannot prevent the rise of stealthy activists using faxes, e-mail, computer networks, etc.

In the years ahead, the possibility should not be overlooked that a major new global peace and disarmament movement may eventually arise from a grand alliance among diverse NGOs and other civil-society actors who are attuned to the doctrinal elements of netwar. They will increasingly have the organizational, technological, and social infrastructures to fight against recalcitrant governments, as well as to operate in tandem with governments and supranational bodies that may favor the movement.

U.S. officials and analysts are accustomed to viewing economic actors and policies as potential instruments for urging foreign governments to move in liberal democratic directions. Transnational civil-society actors whose focus is more informational than economic may prove even more potent as information-age instruments of policy (e.g., "democratic enlargement"). Indeed, many networked NGOs are as transnational as corporations—and they can move faster, too. Chris Kedzie's (1995) work on the positive correlation between political democracy and communications connectivity provides a basis for urging that policymakers begin to treat information as a new dimension of policy and strategy (see Arquilla and Ronfeldt, 1996).




We have shown that network forms of organization (and hybrids with other forms) are spreading among a broad array of actors, strengthening them in ways that present new and continuing difficulties for those who want to control or defeat them. Again, many of these types of actors have deep historical roots, but largely because of the information revolution, they are gaining organizational vibrance, a sense of mission, and an improved robustness against countermeasures.

Some of the types discussed operate in isolation, but often there are cross-linkages. Chechen ethnonationalists, for example, are fighting for the autonomy of their region from Russia; at the same time, Chechens are deeply involved in what is known as the Russian mafia, which has nodes throughout the former Soviet Union, in eastern and central Europe, and even toeholds on both coasts of the United States. Interestingly, Dzokhar Dudayev, the Chechen rebel leader, attempted to deter the recent Russian incursion into Chechnya by threatening an escalation of the conflict throughout Russia, utilizing "forward-based" nodes of the Chechen mafia network as jumping off points for a punitive netwar.

Netwar protagonists will likely range from those that have global agendas and capabilities, to those that are regional or local in orientation, to those that oscillate between global and local agendas. Islamic revivalists seem to fit all these patterns—sometimes they focus on influencing events in specific countries (e.g., in Egypt and Algeria); at other times their endeavors have a regional focus (e.g., Middle Eastern–sponsored efforts in the Levant, former Soviet Central Asia, and the Persian Gulf); and, finally, there are occasions when Islamists try to affect the tone of world politics. An example of this last phenomenon can be seen in the expansive terrorist planning of Sheik Rahman, whose campaign of terror sought to deter American involvement in "managing" the affairs of the international system.

In addition to its attractiveness to terrorists, netwar will likely become a mode of conflict of choice for a multitude of state and nonstate actors. This choice, or tendency, may be fostered by the very preponderance of American power in the post–Cold War world. Simply put, the lopsided victory over Saddam Hussein may have proved that trying to imitate the power possessed by the United States is too difficult. Instead, challenging American preeminence in unconventional ways, such as are afforded by a netwar doctrine, is indicated.

In the future, many adversaries will be transnational, even global, and will have the potential to affect (and perhaps threaten) political and economic aspects of the world system. Such actors may include (in addition to the aforementioned radical Islamic fundamentalist movements and the states that support them): internetted transnational criminal enterprises and information-age social and ideological movements. Other actors may be regional or local, principally including most ethnonationalist movements along with local grievance groups and other insurgents.

There will likely be both vertical and horizontal interactions among them. At the vertical level, global actors may exploit local grievance groups for their own purposes, or vice versa. The Zapatista movement, for example, could be viewed as a local grievance group that has linked up with global human-rights and other activist NGOs in a netwar against the Mexican government.

Another possibility, this time at the horizontal level, is that local groups may connect to other local groups, or global actors to other globals. In waging defensive netwar, it will be useful to understand the nature of the opponent's structural alliances. Coping with a violent local insurgency may be complicated if it has reached out to nonviolent civil society actors for support. The Mexican government is learning this in Chiapas.

Because of the likely profusion of netwars, it may be advisable to begin tracking and cataloging them in all their varieties and locations. This could be undertaken along the lines of annual reports similar to ones that already exist about more traditional modes of conflict (e.g., the volumes by Brassey's and by the Stockholm International Peace Research Institute).

## The United States in the Age of Netwar

- **The United States will benefit from new epoch**
  - **Consolidation of power at global level**
  - **Diffusion of power in and to regions**
  - **Potential new allies among NGOs**
- **The United States will face new vulnerabilities and risks**
  - **Openness, power, and restructuring invite challengers**
  - **The United States may be besieged by multiple netwars**
  - **U.S. allies may also be besieged**
- **The United States is vulnerable whether it is isolationist or globalist**

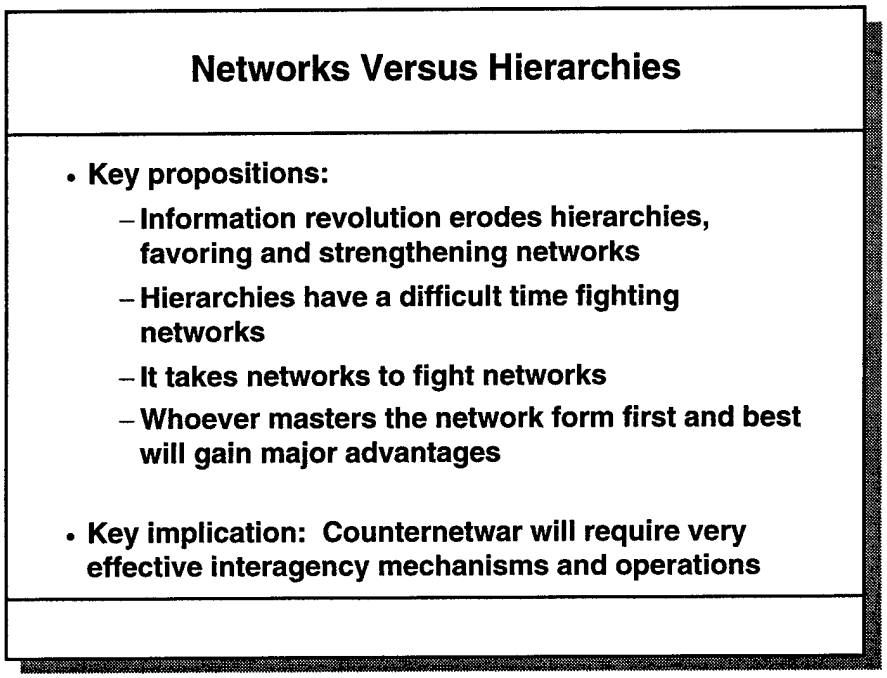
The United States should benefit mightily from the information age. It is moving toward a consolidation of power at the global level; at the same time, it stands to benefit from a diffusion of power in and to actors at the regional level who may be beholden to the United States. As noted earlier, U.S. power and presence around the world should also benefit from the proliferation of potential new allies among NGOs, and from the usage of "information" as a fourth dimension of grand strategy.

Yet, the age of netwar will pose threats, risks, and vulnerabilities for the United States, perhaps more so than for any other advanced society. U.S. openness, one of its greatest assets, becomes a double-edged sword; its very openness as well as its superpower status in an era of restructuring is bound to invite challengers.

As a result, U.S. government and society should expect to be besieged by multiple netwars: leftist and rightist, domestic and foreign, social and criminal, etc. Moreover, U.S. allies may also be besieged, not only in Europe but also in parts of the Middle East and Latin America. We may have to be selective about which netwars to fight, and about which adversaries can most affect our society and security.

U.S. foreign policy, and debates about U.S. foreign policy, tend to oscillate between isolationist and globalist options, with protagonists arguing that the choice can have major effects on our vulnerabilities. Yet, the argument should not be overlooked that the United States will remain vulnerable to netwar whether it opts for isolationist or globalist foreign policies. U.S. society is too interdependent, too interconnected, with the rest of the world for policy orientation at this level to make a major difference, even though once made, the choice may affect the specific mix of vulnerabilities.

Many points we make here are reminiscent of points long made about U.S. vulnerability to international terrorism. Indeed, there may be embedded tendencies in some quarters to react to netwar in terms of antiterrorism models. Those models may be instructive—some terrorist organizations are designed for violent netwar—but they cannot be definitive. Netwar is a broader and a different mode of conflict.




This research on the looming challenge of netwar continues to bear out a set of propositions that we identified some time ago about the information revolution and its likely implications (Arquilla and Ronfeldt, 1993):

*The information revolution favors and strengthens networks, while it erodes hierarchies.* The continued explosive growth of political, business, social, and other networks that benefit societies, as well as of criminal, terrorist, and other networks that threaten them confirm this proposition, as does the concomitant "softening" of traditional statist institutions.

*Hierarchies have a difficult time fighting networks.* Examples of this appear across the conflict spectrum. Some of the best may be found in the generally failing efforts of many governments to deal with TCOs. The persistence of religious revivalist movements, as in Algeria, often in the face of unremitting statist opposition, shows the robustness of the network form, on defense and offense. The Zapatista move-

ment in Mexico, with its legions of supporters and sympathizers among local and transnational NGOs, shows that social netwar can put a democratizing autocracy on the defensive and pressure it to continue adopting reforms.

*It takes networks to fight networks.* The case of the Southeast Asian pirates makes this point well. The first effort to cope with the resurgence of piracy was state-centered and failed miserably. The establishment of a transnational counter-piracy network proved successful in a relatively short time. This proposition may well be analogous to others in military doctrine, particularly that "it takes a tank to fight a tank."

*Whoever masters the network form first and best will gain major advantages.* In these early years of the information age, those adversaries who have advanced at networking (e.g., criminals, terrorists, and activists) are enjoying a marked increase in their power relative to state agencies. While networking once allowed them simply to keep from being eradicated, it now allows them to compete on more nearly equal terms with states and with other hierarchically oriented adversaries. The history of Hamas and that of the Cali cartel illustrate this.

The information revolution is about both technology and organization. While technology innovation is revitalizing the network form, one must not ignore the importance of organizational innovation. Indeed, every information revolution has involved an interplay between technology and organization that affects who wins and loses. For example, a millennium before the printing revolution, the early Catholic Church had a networked organization that confronted and overcame brutal opposition from one of history's most successful hierarchies, the Roman Empire. The Church later developed its own great hierarchies, ironically making it susceptible to dissent as the printing revolution emerged in the 16th century.

Today, those who want to defend against netwar will, increasingly, have to adopt weapons, strategies, and organizational designs like those of their adversaries. This does not mean mirroring the adversary, but rather learning to draw on the same design principles that he has already learned about the rise of network forms in the information age. These principles depend to some extent upon technological breakthroughs, but mainly on a willingness to innovate organizationally.

For U.S. policy, an early implication of our work is that counternetwar will require very effective interagency operations, which by their very nature involve networked structures. It should not be necessary, or desirable, to replace all hierarchies with networks. Rather, the challenge will be to blend these two forms skillfully, while retaining enough central authority to encourage and enforce adherence to truly networked processes. In this manner, states may come to be better prepared to confront the multitude of new threats emerging in this information age.

## Current Interagency Designs Are Instructive . . . But How Adequate Are They?

- **Past difficulty in moving from hierarchical "stove-pipe" to flat "dish" designs in netwar-related areas**
  - **Counterterrorism**
  - **Counternarcotics**
  - **Counterproliferation**
- **New issue areas add to complications, partly because of involvement of activist NGOs**
  - **Peacetime contingency operations**
  - **Computer and cyberspace security**

**Research needed to identify and refine the options for organization, doctrine, and strategy—for domestic and foreign operations**

In recent years, efforts have been made to develop and streamline truly interagency task forces to cope with terrorists, drug traffickers (and other TCOs), and WMD proliferators—all areas replete with netwar-related characteristics. By any set of measures, however, results have proven mixed.

Terrorism has come to America, from the World Trade Center in New York to the Murrah Federal Building in Oklahoma City. Drug flows continue unabated, with production and transshipment sites now being moved to Northern Mexico, closer to the U.S. "market," and imperiling Mexican sovereignty. Information, and sometimes materials, related to the production of weapons of mass destruction and/or their means of delivery are making their way to the unruly corners of the globe.

The United States in defending against these perils, but its defensive efforts are also proving problematic. Aside from the fact that each of these threat areas presents specific, nettlesome problems, U.S. efforts to address them have generally suffered from a resort to hierarchical "stove-pipe" approaches from the top, and bureaucratic "turf battles" from below. There have been well-informed efforts to move to flatter, more heterarchical, and thus more truly interagency, types of designs. But, with notable exceptions, the problems persist.

New issue areas are emerging that also require interagency approaches—and show the problems sketched above are, in a sense, generic.[1] These new areas include peacetime contingency operations and other aspects of OOTW, which increasingly require but have yet to benefit from solid coordination with NGOs, and which are

[1]Our discussion focuses on government, but businesses are taking initiatives analogous to public interagency efforts (e.g., regarding piracy, the International Maritime Bureau).

often hamstrung by the need for consensus among a multitude of powers or transnational bureaucracies (e.g., the United Nations and NATO in the Balkans, 1991–1994).

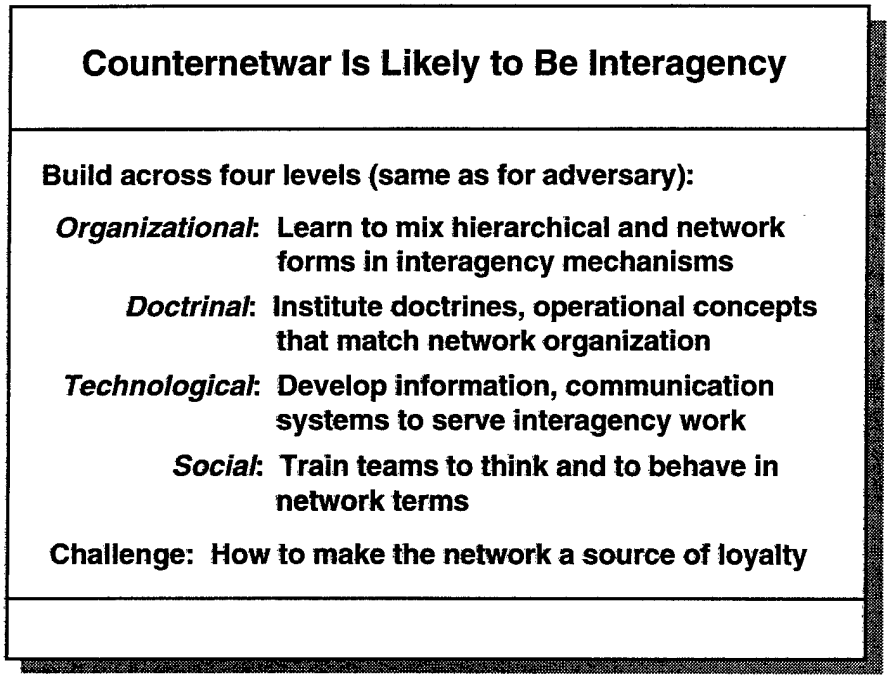
Furthermore, interagency problems are emerging in the area of cyberspace security—likely the next addition to the list. Will bureaucratic politics hamstring government efforts to defend the U.S. (and non-U.S.) "infospheres" from a variety of netwarriors? This possibility has concerned many actors, both in and out of government, all of whom have identified the need for further research into the issues of cyberspace security and safety (Cohen, 1995; Hoffman, 1994; Chairman of the Joint Chiefs, 1993; Libicki, 1994; and Hundley and Anderson, 1994).

All of these areas, from counterterrorism through cyberspace safety and security, are relevant to the netwar phenomenon. Moreover, they all suffer from interagency problems, even though interagency cooperation is imperative in all these areas, and even though U.S. officials have been more successful in some areas (e.g., counterterrorism[2]) than others. What we think would be useful, then, as part of our future research agenda, is to look for ways to prepare for counternetwar by examining, across all areas, what is working well, and what appear to be the best interagency models.

Such research should focus upon organizational matters, to at least the same degree that is often given to the search for technological fixes. For, without attention to organizational design, initiatives to make cyberspace secure will likely fall into a morass not unlike that which has, at times, plagued efforts to cope with terrorism, drug trafficking, and proliferation. The answers to the generic problems of interagency design could come from either of two directions. We could focus on figuring out the lessons for fighting netwars against the TCOs, terrorists, proliferators, and other established adversaries, then apply the lessons to the cyberspace area. Or we could address the cyberspace challenge first and try to derive insights that can be applied to the more traditional areas.

---

[2]Interagency teamwork has reportedly worked better in counterterrorism than the other areas, partly because of the urgency to protect U.S. officials whose lives have been threatened.




An implication that is emerging from our research is that U.S. efforts at counternetwar should be grounded in interagency cooperation (a variant of "jointness"). Preliminary thinking suggests redesigning and rebuilding interagency efforts across four levels—the same levels that apply to a netwar adversary. Again, this does not mean mirroring the adversary, but learning to draw on the same important design principles that he has already learned about the rise of network forms in the information age:

- At the *organizational* level—determining how to optimize the mix of hierarchical and network forms in interagency mechanisms.
- At the *doctrinal* level—instituting doctrines, operational concepts, and strategies that match the interagency approach.
- At the *technological* level—building information and communication systems (e.g., for intelligence sharing) that are interagency in design.
- At the *social* level—adopting new approaches to selecting personnel, and training teams to think and operate in network terms.

A vexing question in all this is how to make the interagency network a focus, and a source, of commitment and loyalty. Comments about past experiences with interagency work in government repeatedly raise the point that the participants tend to treat their home agency, and not the interagency mechanism, as their main allegiance and source of authority. Moreover, they often tend to regard interagency assignments as bad for their careers, compared with a line assignment in their home agency. For interagency approaches to counternetwar to work well, especially when international cooperation is involved, this problem should be resolved. A recent in-

ternational success was scored by U.S., Mexican, and five Central American agencies that shared intelligence and coordinated field actions to strike the hardest (and most successful) blow to date in the drug war.

Exasperation with the operational, bureaucratic, and the various other difficulties of dealing with terrorism, narcotics trafficking, and similar threats, now including those in cyberspace, normally leads to calls to create a "czar" for that threat domain. This may be muted by avowals that, yes, it should be an interagency czar who is skilled at coordinating. But the call—so well symbolized by the very term "czar"—still tends to signify the creation of a hierarchical superior who can centralize disparate activities. And that is part of the problem, as former senior U.S. official Paul Strassmann notes:

> I never understood why everybody called the top man "czar" and not emperor, eminence, lord, majesty, king, pope, kaiser, governor, caliph, shogun, sovereign or shah. I guess that the notorious czarist profligacy, incompetence, inability to govern and dismal endings were the fate to wish on the reigning data center monarchs (Strassman, 1995, p. 479, footnote).

Management literature increasingly makes the point that information-age organizations should move away from hierarchical, centralized designs, toward ones that emphasize heterarchical teamwork (e.g., Drucker, 1993). Some of this literature points out that some multiorganizational problems may be best addressed through informal network designs that emphasize "coordination without hierarchy" (Chisholm, 1989), or designs that are tantamount to what are called "virtual corporations." In this vein, business-oriented literature that talks about the future as the "Age of the Network" puts the focus not on czars but on coordinators:

> [T]he person who makes particular networks happen is the "coordinator." . . . Coordinators appear everywhere in the Age of the Network. . . . Networks began developing new leaders long before computers enhanced their reach. In a richly connected environment where many potential projects are sparking, growing, diminishing, and disappearing, a new role arises, that of the coordinator, whose distinguishing characteristic is the ability to see "connections" among people (Lipnack and Stamps, 1994, p. 173).

Although czar-like leadership may be needed at first to ensure that the members of an interagency network are committed to it, coordinators are ultimately preferable to czars. But if we must use a catchy term, would "khans" not be preferable to czars? Unlike a czar, the Khan ruled with topsight. He saw the "connections" among the diverse, widely separated regions of his dominions. And he took a decentralized approach to leadership, rarely intervening in operations. He was a coordinator as well as a commander.

## Needed: New Research Hubs and Centers

**Observation: It will take rethinking to construct new approaches**

- **Centers for study of organization, doctrine, strategy, and technology to cope with netwar?**
- **Centers for study of "information" as a concept, academic discipline, and military science?**

Learning to counter netwar is no easy task—it will take time, experience, energy, and commitment to build effective approaches to organization, doctrine, and strategy for defending against netwar. The process may be facilitated by establishing special "centers" to advance knowledge about netwar and related phenomena. Some such centers have already been established to develop knowledge about information warfare, narrowly and broadly defined, but more needs to be done in this direction, notably to internet them and to create "hubs."

Our work leads us to propose the establishment of two types of hubs. However, this call for new hubs should not be viewed as traditionalist, as they are envisioned as having limited hierarchical control, even over research agendas. Rather, they would serve primarily as "clearinghouses" for efficiently coordinating ideas, eliminating counterproductive duplication, and bridging the networks of academics, soldiers, and civilian authorities who are already devoting careful, growing attention to the societal and security issues emerging in the information age.

To construct such hubs will still require the formation of new research institutes, or centers. First, because of looming threats and vulnerabilities, it may be advisable to found a strategic institute for the study of netwar in the near future. Such a center should be devoted to both theoretical and applied issues, with the aim not only of analyzing netwars in all their varieties and guises, but also of determining what designs—organization, doctrine, strategy, technology, etc.—may be most appropriate for countering netwars at the societal and military levels.

This strategic institute should strive to provide insights needed to cope with terrorists, transnational criminals, WMD proliferators, and the other networked opponents likely to dominate the "landscape" of netwar. The institute's charter should, how-

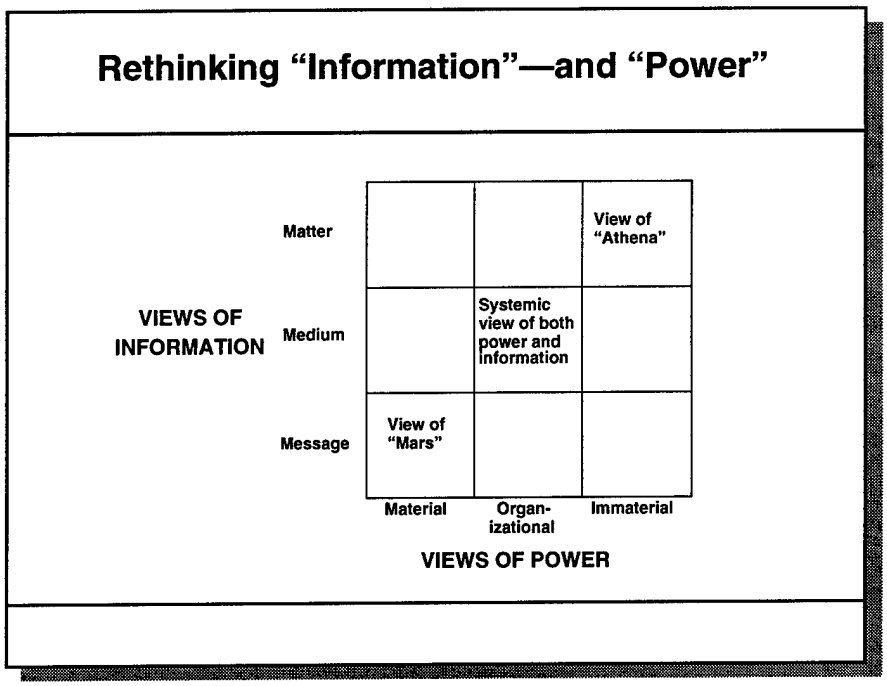
ever, extend beyond areas in which netwar involves significant military dimensions, to include matters relating more to public diplomacy, the protection of intellectual property, and even the modes of academic training most likely to produce a generation of supple-minded netwarriors.

A second type of center, we propose, should be devoted to the study of "information." Indeed, the more we inquire into subjects like netwar and cyberwar, the more we think it may be time for a new academic discipline or field to emerge—Ronfeldt (1992) proposed calling it "cyberology"—as the demands of earlier times resulted in the fields of economics and political science. This center's agenda should extend beyond information science and management to encompass aspects of sociology, political science, economics, psychology, and anthropology. It should draw on the traditions of cybernetics, systems theory, game theory, decision theory, as well as recent theorizing about artificial intelligence, artificial life, chaos, complexity, and information physics.

While the new views about "information" do not fit well into the standard academic disciplines and research fields, extensive intellectual ferment is occurring around the idea that all organized systems, including living organisms as well as societies, depend at their core on how information is generated, transmitted, processed, and controlled. This is leading to an "information-processing view of human organization and society" that means, according to social scientist James Beniger (1986, p. 38):

> [T]he proper subject matter of the social and behavioral sciences, if they are to complement studies of the flows of matter (input-output economics) and energy (ecology), ought to be information: its generation, storage, processing, and communication to effect control.

Such a discipline may sound odd and too diverse, for it would span topics that analysts do not normally group together. Yet this diversity may embody as much coherence as any other academic discipline or field of research. University and other centers might be well advised to develop research capabilities in this respect. Policymakers and practitioners in Washington and elsewhere, at home and abroad, will have an increasing need for analyses that sort out and assess the issues raised not just by the spread and use of new information technologies, but also by what the concept of "information" is going to be all about, in military as well as broad societal terms.




This chart summarizes our point that concepts about "information" and "power" are in need of rethinking.[3]

As depicted above, three views of "information" appear in discussions about the information revolution. Two are widespread: The first views information in terms of the inherent *message*, the second in terms of the *medium* of production, storage, transmission, and reception. An emerging third view transcends the former two; it speculates that information may be a *physical property*—as physical as mass and energy, and inherent in all matter.

Meanwhile, three views of power can also be discerned that parallel these views of information—but with a reverse twist. These three views treat power, respectively, as being material, organizational (or systemic), and finally immaterial in nature. This applies to whatever strategic realm one is analyzing: political, economic, or military, all of which have material, organizational, and immaterial, ideational bases.

These considerations alter the adage that "information is power." We see that "information," generally thought to be immaterial, is increasingly seen to be a tangible part of all matter, while "power," long thought to be based mainly on material resources, is increasingly seen to be essentially immaterial, even metaphysical in nature. As information becomes more material, and power more immaterial, the two concepts become more deeply intertwined than ever.

These trends generate some implications for the theory and practice of warfare and for grand strategy in the times ahead. The three views of power, rotated against the

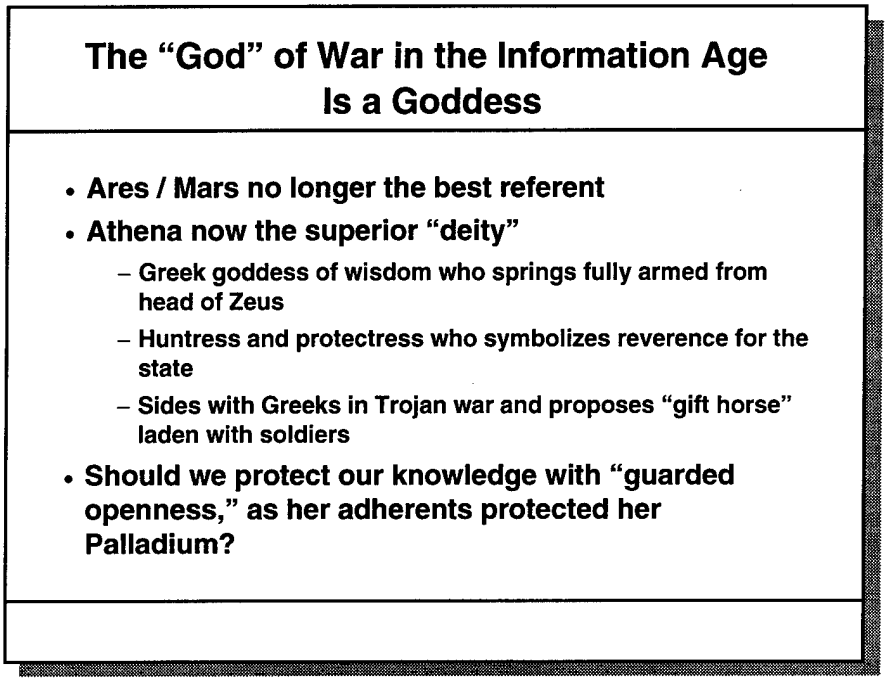
[3]The text for this and the next chart is summarized from Arquilla and Ronfeldt (1996).

three views of information, lead to a matrix of combinations. Three cells are notable. When power and information are viewed in their traditional senses—with power depending on material capabilities, and information being but a useful adjunct—we liken them to Mars, the Roman god of war. We identify Athena, the Greek goddess of warrior wisdom, with the far cell, which corresponds to power and information viewed in postmodern, information-age senses—here information is physical and power immaterial, and the two dynamics merge. In between, on the diagonal, is a cell in which sociosystemic views of information and power coincide. This may well be how many people think today about information and power, and most them are as yet unaware of the Athena cell.

A military force whose doctrine is built around an Athenan view should be able to defeat one built around a systems concept, and it in turn should be able to defeat one built around a Mars view. In general, a cell should represent a stronger approach than any cell beneath and/or to the left of it. This depiction parallels Martin Van Creveld's (1989) view of military history, wherein he traces the evolution of war in terms of its being based first on the tools and materials of war, second on systems of warfare, and third on information-based technologies like the computer.

Which views or blends of information and power one prefers affects how one proceeds to think about the implications for warfare. We presume that thinking about information and power is moving in the "Athenan," direction. More to the point, the Athenan view of information and power implies targeting whatever represents or embodies the most information on an enemy's side. This implies ascertaining and attacking the most information-rich components of an adversary's order of battle, a point that applies across the conflict spectrum.

An example of an implication for netwar is that counternarcotics operations should focus on attacking traffickers' electronic funds transfers and other financial transactions, rather than trying to chase smugglers or eradicate crops that represent lower information content (Andelman, 1994). Another implication of the Athenan viewpoint is that the information age will raise the value of social and human capital, since man remains the purest, richest information system.




Metaphors and analogies can help convey new concepts like netwar by providing simplified images that work to encapsulate complex points. We provide two such metaphors or analogies in this briefing. The one raised here contrasts Mars and Athena as gods of war. The other, raised near the end of the briefing, contrasts chess and Go as paradigms of war.

Information has been associated with power, war, and the state since at least the time of the Greek gods. One normally thinks of Ares, or the Roman refinement Mars, as the god of war. But where warfare is about information, the superior deity is Athena—the Greek goddess of wisdom who sprang fully armed from Zeus's head and became the benevolent, ethical, patriotic protectress and occasional wrathful huntress who exemplified reverence for the state.[4]

According to Virgil, Troy would be powerful enough to withstand all its enemies so long as it possessed and honored the Palladium, a sacred statue of Athena provided by Zeus or Athena herself. Understanding this, the Greeks arranged to steal the Trojan Palladium, symbolically denying the Trojans the benefits granted by access to the goddess of wisdom. As a result, Athena sided with the Greeks in the Trojan War, where she bested Ares on the battlefield and conceived the idea of the wooden "gift horse" secretly loaded with Greek soldiers. The Trojans made the monumental misjudgment of hauling it inside their fortress, over the protestations of the priest Laocöon and the seer Cassandra. The rest is history, and legend—and ever since, ex-

[4]Standard sources on Greek and Roman mythology include Graves (1960) and Hamilton (1969). While Ares is refined by the Romans into Mars, Athena became Minerva. But given the Roman's penchant for specializing their gods, Minerva is mainly a goddess of wisdom, stripped of the warrior element. Thus she does not fit our purposes here.

amining the relationship between information and power has attracted all manner of political and military theorists.

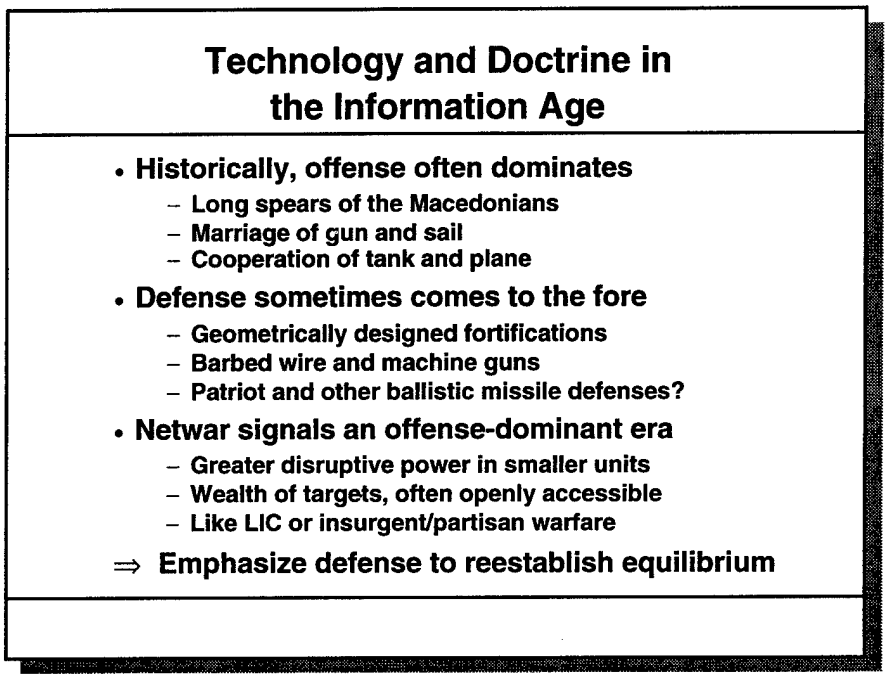
Shifting to view Athena, rather than Mars, as the emblematic god (or goddess) of war in the information age is consistent with Clausewitz's prediction that knowledge would become capability. This shift has more than symbolic import, for it implies that we must begin to think about information as something that may have to be protected. In some ways, this notion runs counter to traditional Western democratic ideals about maximizing openness.

Besides urging that information and communications be treated as a new fourth dimension of grand strategy, our admonition is that U.S. strategic choices be reviewed across the spectrum of alternative approaches to openness. That spectrum might be framed by complete openness at one end and by preclusive security at the other. Something that might be called "guarded openness" would define the middle range of the spectrum.

Guarded openness was, in many respects, the strategy that the United States pursued during the Cold War, if not before. But it is not a static strategy—moreover, it has not even been discussed much as a strategy. However, for dealing with the present and future world, the overall profile of when to be open and when closed should be based on different principles from those that governed strategic judgment during the Cold War, especially given the decline of Russian power and the worldwide diffusion of power to a multitude of smaller actors, many of them of the nonstate variety.

If a high-level policy review were undertaken, it could help to ascertain what contextual factors are most important in determining whether to move in open, guarded, or sometimes preclusive directions in specific issue areas. Such a review would further help identify the mechanisms that should be emphasized for purposes of enhancing and protecting U.S. openness, whenever feasible. Finally, the review process could lead to the formation of national and international "knowledge strategies," in areas ranging from military innovations to commercial intellectual property.

# IMPLICATIONS FOR U.S. DOCTRINE AND STRATEGY




In prior eras of military innovation, technological and doctrinal improvements tended to favor either the offense or the defense. For example, nearly doubling the length of the infantry spear (to 16 feet) gave Alexander's Macedonians incomparable advantages in open battle. When wedded to the doctrine of the phalanx, it generated sufficient offensive power to conquer the known world in a very short time. In the late middle ages, the *trace italienne,* a fortification scheme based on advanced construction techniques and a geometry-based doctrine of creating mutually supporting strong points, gave similarly substantial advantages, but this time to the defensive. Later, the combination of gun and sail gave Western Europeans the ability to exert a centuries-long dominance around the world. In the machine age, the internal combustion engine made tanks and planes possible, eventually inspiring the blitzkrieg doctrine that ended the defensive dominance of artillery, barbed wire, and machine guns. The list is as long as history, up through and including recent developments in ballistic missile defenses (BMD).

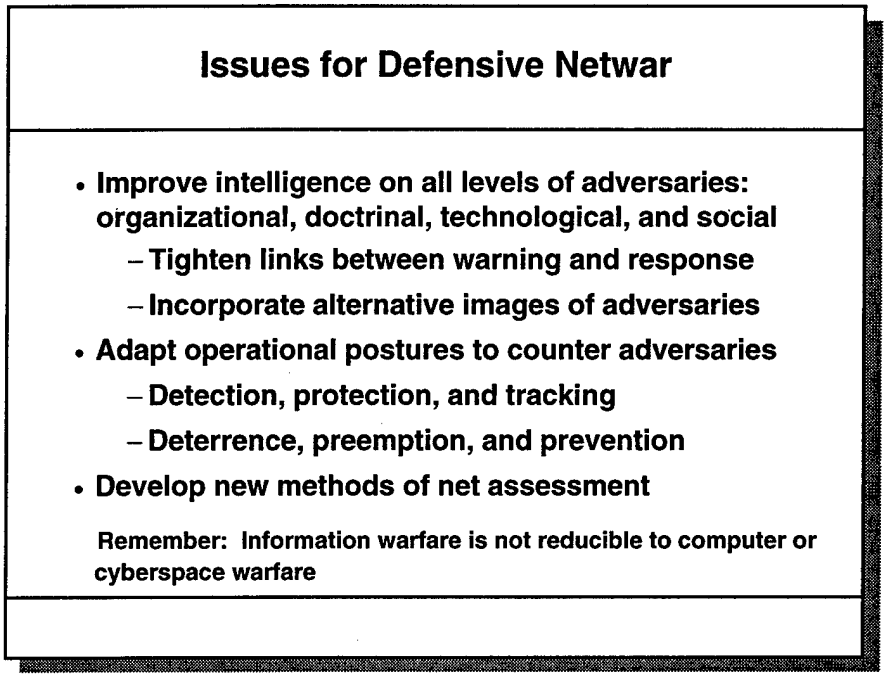
More recently, mutual nuclear deterrence equated to the superiority of the defensive. However, at the low-intensity end of the spectrum, innovative approaches to revolutionary warfare created tremendous opportunities for the weak to attack the strong, much as North Vietnam challenged American might in the North's campaign of conquest against the South.

In the information age, what will be the case? We anticipate that netwar will resemble low-intensity conflict (LIC) more than nuclear or high-intensity conventional warfare; that it will have many of LIC's offense-dominant attributes. If this is true, there is a pressing need for new doctrinal insights to revivify deterrence and defense. However, it may be that deterrence against netwar will grow problematic, and all that will remain is a choice between either preclusive or depth-oriented defensive schemes. The former implies an ability to provide "leak-proof" defenses, while the latter accepts initial incursions, then aims to expel the intruders or invaders by means of counterattack.

These strategic choices mirror, in many ways, the problems facing the German High Command in the spring of 1944 in Western Europe. Field Marshal Erwin Rommel took a preclusive approach, urging the use of all 60 divisions available to prevent the establishment of an Allied lodgement on the continent. His immediate superior, Field Marshal Gerd von Rundstedt, championed the notion of forming a depth-oriented reaction force that would allow initial landings, then fight a decisive battle of maneuver in the French countryside. After months of fractious debate, Hitler chose a bureaucratic compromise between the two, which made neither approach feasible.

Whatever strategy (or hybrid) is employed to defend against netwar, the age-old cycle of action and reaction between offense and defense appears to be under way again. The path to a new equilibrium is not yet clearly mapped out, and choices made now will have lasting, powerful effects.

The next two charts and their texts begin to address some strategic and doctrinal issues that the U.S. government may face if it has to prepare to defend against netwar actors who may be violently aggressive toward the United States. The supposition is that such actors, by combining aspects of Hamas and the Legion of Doom, would attack through both cyberspace and irregular military (or paramilitary) means. Thus, the text about these two charts does not apply to activist NGOs, though the subsequent charts comparing chess and Go as paradigms of conflict do apply broadly to all varieties of netwar actors.




From the American perspective, it seems clear that a key issue will be to move expeditiously toward the development of capabilities for waging defensive netwar. Thankfully, the immediate post–Cold War period has brought a substantially lessened nuclear threat (though it does persist), and U.S. conventional forces enjoy a preeminence seldom seen in world history. The same cannot be said of U.S. preparedness for netwar. Indeed, without sounding unduly alarmist, we feel it necessary to warn of the possibility of a "netwar gap" that sees U.S. adversaries in possession of relatively greater capabilities for waging this lower-intensity form of warfare.

Counternetwar will require intelligence of a type different from that which was most useful during the Cold War. Counting tanks, guns, planes, and other such weaponry must give way to developing information about a potential adversary's organizational structures, the better to be able to target his key nodes. Threat assessment will naturally involve examining an adversary's capabilities *and* intentions. However, intelligence may have to shift from the Cold War focus on capabilities to giving primary attention to intentions. During the period of U.S.-Soviet rivalry, it was prudent to hedge, keeping the adversary's capabilities uppermost in mind, particularly because intentions could not be discerned easily. In the information age, the "intentions side" of the equation has become even less clear, but more important—especially since the societal aspects of netwar revolve more around the less tangible power of ideas and of networked organizational structures. However, since netwar aggression will often be accompanied by an open declaratory policy (e.g., political independence or respect for human rights), there may also be new opportunities for generating insights into intentions.

Improved intelligence may also be needed to help couple warning and response more tightly. As opposed to the Cold War situation in which possession of survivable

second-strike forces enabled the superpowers to eschew doctrines of "launch on warning," in netwar, by the time warning is received, great damage may already have been done. Thus, it may be incumbent upon decisionmakers to move with dispatch on the basis of warning, and it is vital for intelligence gatherers to provide real-time information as little susceptible to ambiguous interpretation or misconstruction as possible.

In netwar, the attacker may often be difficult to identify. To deal with this ambiguity, defenders may find it useful to use an approach that provides alternative images of the attacker. This analytic framework enables the defender to construct and assess well-hedged defensive strategies, even when uncertainty about the attacker's identity persists. If, for example, it is unclear whether the attacker is a disgruntled individual (a Unabomber), a small group of malcontents (most likely the case with Sheikh Rahman and his adherents), or a full-blown terrorist organization, perhaps with state sponsorship, then considering the possibility of any of the three being the attacker will usefully inform the search for countermeasures (see Davis and Arquilla 1991a, 1991b). This hedged approach, which relies upon alternate imaging of the adversary, may help to prevent overreaction against minor miscreants. However, this approach may also make it much harder to arrive at decisions to retaliate massively against more serious attackers and/or putative sponsors whose identities have not been established beyond doubt. Indeed, this problem of ultimate identification may be a central security dilemma posed by the advent of netwar.

In tactical, or even operational, terms, defensive netwar will be concerned with three functions: detection, protection, and tracking. Briefly, the ideal in detection would be to gain awareness of an attacker before an incursion is made (either in cyberspace or in terms of some nascent societal-level movement). Practically, however, absent outstanding intelligence about enemy intentions, detection will more likely occur only after an attack has begun. With this in mind, protection will become a key operational task in defensive netwar. Damage limitation will be a primary goal and may be pursued through efforts at preclusive security (e.g., by "firewalls," or by raising public awareness of the nature of the opponent and its aims), or by allowing the attacker some "running room," then tracking him down.

Clearly, the greatest operational emphasis in defensive netwar must be protection. Understanding one's own key institutional nodes is crucial, because defensive robustness will revolve around either the protection of such nodes or the development of redundancies to mitigate their potential loss. Presently, the amorphous nature of the offensive netwar threat makes for an unwillingness to incur the expenditures necessary to provide such protection. Indeed, the situation is not unlike that along the eastern U.S. seaboard during the first months after American entry into World War II. The nature of the U-boat threat was not yet fully understood, and there was an unfortunate practice of allowing port cities to remain illuminated at night. This created something of a "happy time" for German submarine captains, since leaving the harbor lights on allowed them to acquire well-silhouetted targets easily. At present, the netwar threat poses a new "harbor lights" problem, in cyberspace and in the real worlds of government, commerce, and society. For example, there is too little encryption of important military, scientific, and commercial/financial data, and

too much intellectual property readily identifiable and accessible to those who might use such information malevolently.

At the strategic level of analysis, three major concerns of defensive netwar are deterrence, preemption, and prevention. The first relates to the conditions under which an adversary will be dissuaded from launching a netwar offensive. Preemption only comes into play when the defender believes an attack is coming and decides to strike first to avoid or weaken the offensive blow. Finally, prevention seeks to cripple potential netwar adversaries *before* they develop their offensive capabilities. Each of these three strategic perspectives has merits, but also problems, some quite serious.

A deterrent strategy is the most purely defensive in nature. However, a problem with effecting it is that the intelligence requirements for detecting an immediate netwar threat are huge. Even if signs of an impending attack are uncovered, there is a strong possibility that the true identity of the aggressor will be shielded. These problems should lead us to infer that successful deterrence under conditions of uncertainty may rely, ultimately, on the development of protective (i.e., preclusive as well as damage-limiting) measures that serve to convince a potential attacker that the defense can *deny* him the achievement of his aims. This is contrary to Cold War–era deterrence, which relied heavily on *punitive* threats to keep the peace.

Because of the difficulties in correctly identifying a netwar attacker, "denial deterrence" may now have to come to the fore. However, there will no doubt be occasions when the attacker's identity is clearly established. In these situations, retaliatory punitive action would seem appropriate so as to provide a dissuasive example for other would-be attackers. But what if the attacker strikes at some key aspect of the U.S. information infrastructure and has no similar set of targets of his own that can be held at risk?

An answer to this problem is that retaliation need not be in kind, though proportionality ought, in general, to be the goal (Schelling, 1966). A nuclear response to a state-sponsored attack in cyberspace is wildly disproportionate, but precision bombing of enemy intelligence or other military facilities would likely be appropriate. Depending on the clarity of the evidence identifying the attacker, and the attendant international political costs of a disproportionate punitive response, there may also be occasions on which a kind of "massive conventional retaliation" can be carried out. In such instances, disproportionate responses may have lasting deterrent effects on both the attacker in question, and upon other potential attackers.

Because of the subtle nature of netwar, which makes even deterrence problematic, the prospects for developing a successful preemptive strategic doctrine seem slight at this time. Technical constraints aside, the political costs of preempting, based even on the most compelling indicators, could be enormous. Netwar does not require lengthy mobilization processes common in other forms of warfare. This difference may leave an aggressor in the position of being able to deny plausibly that he ever intended to attack. However, if intelligence indicating an attack is strong enough, decisionmakers will need to weigh the political costs of preemption against the damage likely to be incurred in the netwar attack. There may well be times when preempting, then taking the international "heat," is the optimal course of action.

Preventive defensive netwar is perhaps the most controversial strategy, because it implies a willingness to keep a potential adversary from developing offensive capabilities. If the political costs of preemption are high, then the price of prevention is likely to be astronomical because, operationally, it will look much like attacking an innocent bystander. However, preventive netwar might also consist of measures scarcely detectable, such as maintaining a "forward presence" inside an information infrastructure, or inside a particular societal or political movement. The implication here is that having preventive netwar as a policy option may require considerable capabilities for intelligence collection and for covert action, an issue that raises political, administrative, and legal questions (see Reisman and Baker, 1992).

## Will Paradigm Shift Be Required?

**In a world of netwars, where boundaries are blurred between peace and war, and offense and defense:**

- **How will threats be assessed?**
  - **What will determine and set priorities?**
  - **Will we have to select which netwars to counter?**
- **Will defense or offense predominate?**
- **What will be key new considerations for strategy?**
  - **Linear vs. nonlinear**
  - **Sequential vs. cumulative**
- **Will netwar reflect Sun Tzu more than Clausewitz?**

In the emerging information age, the conduct and context of conflict are undergoing radical transformations. Indeed, the multidimensional nature of netwar makes it ever more difficult to demarcate clearly between peace and war. For example, the rise of a politico-military movement, like the EZLN in Mexico, may signal the opening of a netwar for control of the state, even in the absence of ongoing military operations to seize the state. Or, as in Colombia, state institutions may be compromised or kept under siege by TCOs as part of their day-to-day operations.

Many netwar actions and operations, with regard to offense or defense, are observationally equivalent. Thus, preemptive or preventive actions of a tactically or strategically defensive nature may actually be perceived as offensives. But the reverse may also be true, in that some offensives may not appear as such, weakening the linkage between warning and response. This is quite different from more traditional types of warfare. For example, a conventional blitzkrieg features fast-paced, well-integrated combined-arms operations and is clearly recognizable as offensive. In contrast, netwar actions, such as degrading an opponent's communications structures, may be either offensive or defensive, or both.

Because netwars are easy to start and wage, there may be many of them going on all of the time. The average number of conventional wars in progress since 1990 has been about 30 (see Brassey's 1991–1994; and Stockholm International Peace Research Institute, 1991–1995). We should expect the number of netwars to increase by an order of magnitude.

This likely profusion of netwars implies a need for prioritization, and for a new calculus of intervention. It is not clear that the public-opinion-oriented criteria of the Weinberger Doctrine (1984) still apply, given that the early stages of intervention,

and perhaps the later ones, will often take place outside the public's knowledge. Also, victory in netwar may not resemble the winning of more conventional conflicts and may defy easy definition or characterization.

Public support and high probabilities of winning aside, some of the Weinberger Doctrine's other guidelines also seem problematic when applied to netwar, particularly its requirement that clear military and political objectives be present from the outset. In counternetwar, clarity may not be achieved for a long time, since attackers will often mask their ultimate objectives as long as possible. To require clarity as a prerequisite for intervention would be to debilitate defensive netwar from the outset.

Perhaps what is needed is a broader, but still practically useful, set of measures for prioritizing interventions. Perhaps Mill's (1857) admonition to limit involvement to countering others' interventions is a good starting point. However, even this limitation to waging counternetwar defensively is likely to leave an overabundance of potential cases for involvement. The best solution to this dilemma may lie in developing a fully articulated methodology for assessing netwar threats, one that would perform a strategic-level *triage.*

One category of triage, the most urgent, would be for cases requiring immediate action, lest some U.S. friend or interest suffer grievous harm or loss. U.S. economic and even military cooperation with Mexico to deal with major, violent instability along the border or to intensify the fight against drug cartels could fall into this category. A second class of cases might contain those in which the victim of netwar may suffer but is likely to ultimately prevail on its own (e.g., Russia's current fight against Chechen guerrillas and criminal elements). Finally, there will always be some set of cases where the costs and risks of intervention in a netwar will outweigh the plausible benefits. Avoidance might be the advisable stance for these (e.g., the ideological, social, and military struggle for control of Algeria).

Despite all the blurring between war and peace, and between offense and defense, the question still stands as to whether offense or defense will predominate in netwar. The advent of netwar is similar to the rise of earlier forms of conflict in that offensive action is initially the easier, and more likely successful, tack (Quester, 1977). This is one reason why U.S. policy faces a challenge in having to emphasize defensive netwar—with the goal of reestablishing an equilibrium between offense and defense.

Strategically, netwar appears to depart from earlier modes of conflict in that it is nonlinear. In the past, warfare and other forms of conflict have tended to follow linear, sequential patterns based on geographically derived aims. Now, in place of linearity and sequential objective-seeking, netwar may be waged anywhere, at any time. Victory will come not so much to those who reach some geographical objective, as to those whose efforts accumulate a set of advantages. Thus, the Mexican military's occupation of Chiapas may have been more than offset by the EZLN's gains in mustering NGO support for its reform agenda. In this case, a territorially oriented counterinsurgency was outflanked by a movement well aware that the netwar "battlespace" extended far beyond the limits of a remote southern state of Mexico.

In the metaphor of board games, the aim in netwar is not for checkmate, as in chess, but rather for control of more of the continuum of conflict, as in Go. Interestingly, Wylie's (1967) visions of cumulative versus sequential strategies offered early, prescient insights into the likely future of conflict. Also, some theorists of nuclear strategy were, because of the nature of the weapons they considered, strategically steeped in both nonlinear and cumulative notions (Kissinger, 1957; Kahn, 1960).

Go, a product of the East, may offer more insights than chess, the favorite of the West. So Western strategic thought, as epitomized by Clausewitz and Jomini, may have to give ground to Sun Tzu, the great Chinese strategic thinker. One key difference between the two is that Clausewitz tended to downplay the importance of informational factors, believing that the problem of "friction" would vitiate any advantages won by means of a "knowledge strategy" (see Handel, 1991). Sun Tzu, however, held that information dominance was crucial to victory, tactical or strategic, and that control of information could create a condition of "entropy" in the opposing camp.

Sun Tzu also held that the key to victory lay more in position than maneuver, arguing that the possession of key points (not "fronts" but points) could lead to victory even in the absence of battle. This idea runs counter to Clausewitz's view that victory could only be won through an unflinching willingness to engage in bloody fighting for territorial dominance.

In the information age, Sun Tzu may thus provide a more appropriate foundation for the development of a new strategic paradigm. Just as in many areas of activity, a "Pacific Century" is emerging, so key advice for strategic thinkers may be, "go East" (as opposed to Horace Greeley's advice to go West).

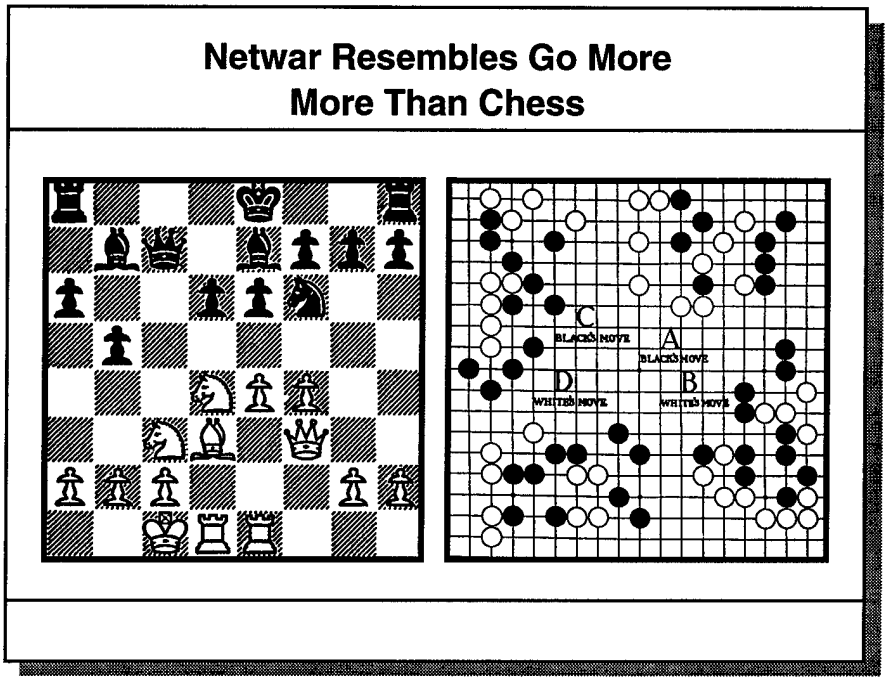
Previous views of history have inclined toward a view of conflict as dual in nature. For most, warfare is either positional or maneuver-oriented (Liddell Hart, 1954). Hans Delbrück (1900) also adopted a dual definition, contending that conflict was of two types, either "exhaustion" or "annihilation." He noted the Periclean strategy at the outset of the Peloponnesian War as a key example of attritional warfare; he saw the campaigns of Napoleon as the apex of "decisive battle."

More-modern examples of these two types of war abound. World War I was certainly fought to exhaustion, and the major limited conflicts of the Cold War–era (Korea and Vietnam) and numerous civil wars (from Guatemala to Angola) were clearly attritional in nature. World War II, however, was decided by great annihilational battles (Stalingrad and Normandy, in particular); and many internal wars have aimed at the utter destruction of one side, as can be seen in recent societal conflicts, from Bosnia's "ethnic cleansing" to the outright genocide that took place in Rwanda.

In our view, a new paradigm for conflict is needed that incorporates the various implications of the information age. Broadly put, conflict may be moving beyond attrition and/or annihilation to a new phase in which "information dominance" (Arquilla, 1994) may allow for victory through *disruption.* In the future, it may be likely that forces disrupted cannot fight with any degree of effectiveness. Certainly the Persian Gulf War provides an example of a very large, well-armed military that was almost completely disrupted because of strikes at its key communications nodes.

Victory was achieved at very modest cost, relative to the comparative historical experience of other wars.

Next, using our game metaphors, we explore further these notions of the blurring of offense and defense, nonlinearity, cumulative strategy, and disruption as a new "third face" of conflict. The following discussion of chess and Go is drawn from Arquilla and Ronfeldt (1996).




As in the past, war and other modes of conflict in the information age will continue to bear resemblances to the game of chess. But such conflicts will increasingly take on characteristics of the "double-blind" chess variant *kriegsspiel* and of the very different Japanese game Go. If chess or *kriegsspiel* were played so that one's own side has sight of both his and his opponent's pieces, but the opponent can see only his own pieces, then we would have an analogy for military "cyberwar." For an analogy for social and other types of "netwar," we would play Go so that, again, one's own side sees all pieces but the opponent sees only his own pieces.

In chess, each side has a king and five other types of specialized pieces. Each piece, including the king, has a different "value" and a different ability to move. Each side lines up its pieces in assigned positions on opposite sides of the game board. Thus the two sides face off across a "front line." Then, each side maneuvers in ways that are generally designed to fight for control of the board's center, to shield one's valuable pieces from being taken, to use combinations of pieces selectively to threaten and capture the opponent's pieces, and ultimately to achieve checkmate (decapitation) of the one-and-only king. Warfare before World War II was often like this and, indeed, frequently continued to retain this linear flavor up through the Persian Gulf War.

For the age of cyberwar, a modified *kriegsspiel* analogy is more apt. *Kriegsspiel* is based on chess—the board, the pieces, and the rules are similar—but the game is operationally distinct. Each player has his own board and arrays his pieces as in chess. A screen to block vision stands between the two boards, manned by a monitor (referee). Thus, once the game starts, each player knows where he has moved his pieces but cannot see, and must guess based on limited information, where the other player moves. The monitor signals when contact is made. Then, whoever's turn is

next gets to choose whether to take the contacted piece or make another move. He does not see what piece he may take until he has taken it, and it is handed to him by the monitor.

Throughout the game, each player speculates but rarely knows which of the opponent's pieces are where. The game revolves around information vacuums and uncertainties. A premium is placed on deception. Indeed, a player who opens with classic chess moves and strategies—e.g., controlling the center—is likely to lose. (The edges of the board may become more important for maneuver than the center.)

The aim of cyberwar is for its side (the United States) to play chess—i.e., to have full sight of its own and the opponent's pieces—while blinding the opponent so that it has to play *kriegsspiel*, at best knowing the location only of its own pieces, and maybe not even that. In this analogy, both sides start with similar mass and energy—the same set of pieces—at their disposal. But the U.S. side has an enormous informational advantage—what David Gelernter (1991) calls "topsight"—and because of this, each of the U.S. pieces is well informed. This advantage means that the United States should not require as many pieces to win; it might even be able to achieve checkmate without taking many of the opponent's pieces. The Persian Gulf War was, in some respects, rather like this and marks a watershed in the transition from traditional attritional warfare to a new generation of information-age warfare.

## Strategic Characteristics of Go Differ from Chess

- Go starts with empty board
- All pieces ("stones") are identical—unlike specialization in chess
- No preassigned starting positions; multilinear opening moves
- Primary aim is to surround territory—taking pieces is secondary
- Decapitation not posssible—no "king" in Go
- Control of corners and edges precedes control of center
- Presence is more important than maneuver—distributing pieces is more important than massing them
- Defense and offense blurred
- Success depends on lines of communication to link pieces
- Go ends with full board; winner has largest secure territories

The game of Go provides a better analogy for netwar, i.e., for networked types of conflict and crime at the opposite end of the spectrum from high-intensity conventional warfare. Whereas chess starts with all pieces on the board, this game starts with an empty board. It resembles a vast, grid-like chessboard with lots of tiny squares. Each side takes turns placing pieces called "stones" anywhere on the board, one by one. But the stones are placed not in the squares as in chess, but on the points where the grid lines intersect. All stones are alike—there is no king to decapitate, and no queen or other specialization.

Once placed, a piece cannot move; it can only be removed, if surrounded and captured according to the rules. But in this game, taking pieces has secondary importance. The goal is to surround and hold more territory than one's opponent. Once emplaced, a piece exerts a presence in that part of the board, making it easier for the player to place additional pieces on nearby points in the process of surrounding territory. As a result, there is almost never a front line, and the major battles are less for control of the center than for the corners and sides (since they are easier to box off). And whereas in chess no piece is ever totally secure, in Go a piece of territory can be made totally secure if it is surrounded in a particular way (in Go parlance, given two "eyes").

Thus Go, in contrast to chess, is more about distributing one's pieces than about massing them. It is more about proactive insertion and presence than about maneuver. It is more about deciding where to stand than whether to advance or retreat. It is more about developing web-like links among nearby stationary pieces than about

moving specialized pieces in combined operations.[1] It is more about creating networks of pieces than about protecting hierarchies of pieces. It is more about fighting to create secure territories than about fighting to the death of one's pieces. It is also less linear than chess.

Go analogies appear at times in high-intensity, conventional conflicts. For example, the World War II Battle of the Atlantic had many of the game's characteristics. Moves—attacks—were made all over the board (the seas) from day to day, and secure areas in the battlespace were developed first around the edges (the European and American coastal seas), and later extended to protect convoys throughout their voyages. Victory in this campaign depended upon the cumulative results of the fighting (merchant ship production less losses versus U-boat production less losses), rather than upon the achievement of some sequential, territorial objective.

Yet, Go is far more like social, criminal, and revolutionary forms of low-intensity conflict than like full-scale military war. It might even be said that the forces of North Vietnam and the Viet Cong played Go while U.S. forces tried to play chess (Boorman, 1969). In line with this analogy of Go with irregular warfare, the game's tactics are very unforgiving of efforts either to build fortifications or to seize unclaimed territory. Bastions or redoubts are subject to implosive attacks that bring them down from within, while "ground taking Go" is quite predictable, allowing a smart adversary to ambush these interspersed forces, defeating them in detail.

Finally, we note that the comparison of chess and Go speaks to another distinction that may prove increasingly significant in the information age: the distinction between "vital" and "strategic" interests. Chess is mainly about vital interests, particularly in the opening—notably, the security of the king, and control of the center. As the game progresses, the interaction of black and white pieces (forces) creates additional, strategic interests, which may or may not concern the center or the immediate vicinity of the kings. Go, on the other hand, *begins* with only strategic interests—a player has yet to determine where to stand, attack, or disconnect. Only later, as the board fills with black and white forces, do vital interests emerge, often according to which portions of the board seem to develop greater or lesser degrees of importance to the outcome of the contest. As the world grows more interconnected, it is incumbent upon the United States to attend to the distinction between vital and strategic interests, and to the possibility that the strategic ones will grow in significance relative to the vital ones.

---

[1]The extension of a piece into a line (a chain network?) might be a form of maneuver.

## Game Is Even More Like Netwar If One Side Has to Play Blind

- **Information warfare is about who knows what and when**
  - **In *kriegsspiel*, both sides are blinded**
  - **What if one side gets to play chess, while other side has to play *kriegsspiel*?**
  - **And what if this is applied to Go?**
- **If one side is kept blind, then side with "topsight" has the best-informed pieces**
  - **The side with topsight will surely win**
  - **It can do so even if it starts with fewer pieces**

The metaphoric possibilities for netwar deepen if one imagines combining Go with the key characteristic of *kriegsspiel*: the screen that obstructs sight. Again, presume that one side has full knowledge of its own and the opponent's array, but the opponent can see only its own pieces until contact is made with an opposing piece. The dynamics of Go differ from those of chess/*kriegsspiel*, but the point still stands: Both sides start play with virtually equivalent mass and energy at their disposal. But the side with topsight has far more information. Thus, it should win handily over a blinded player and require (or need to risk) far fewer pieces to do so.

It might be illuminating to run experiments about this point, not only to test its validity, but also to see whether a minimum essential force size can be defined that invariably wins at chess/*kriegsspiel* or Go so long as its side has topsight and the other side is blinded. The experiment could vary the amount of information available to either side to see what types and thresholds of information may make the most difference.

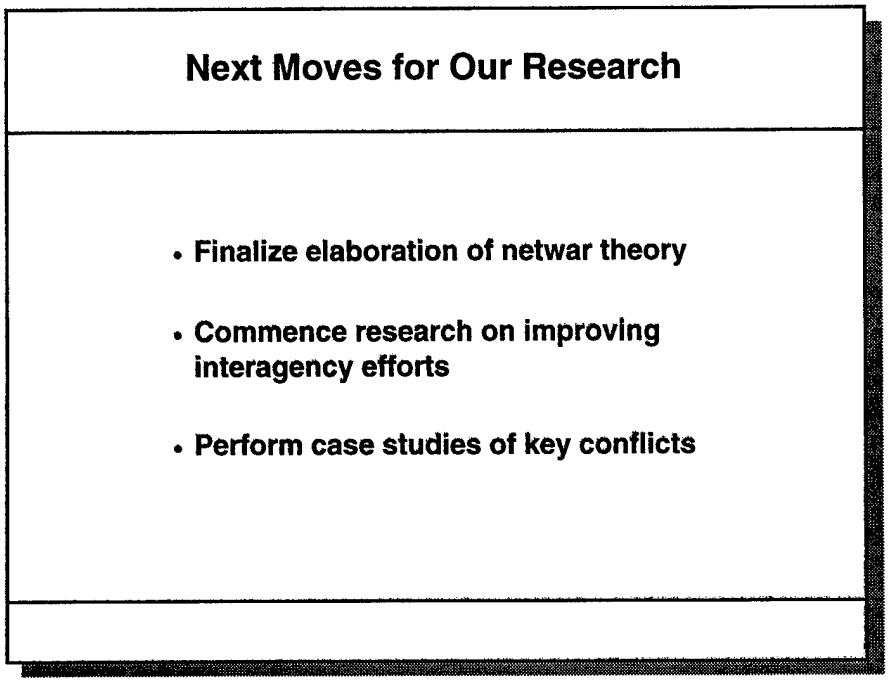
To refer to the well-known "information pyramid," which features wisdom at its narrow top and raw data at its broad base, it might be found that a game will turn in favor of whoever has better knowledge and wisdom, so long as both sides have full view of the board. But the more one side is blinded, the more the game may turn simply on who has the most data and information in the narrow senses.

In addition, it might be illuminating to identify for study a series of cases in which apparently small, weak military forces effectively defeated or defended against what appeared to be much larger, stronger forces. The offensive skill of the Mongol "hordes" of Genghis Khan (which were anything but hordes) comes to mind, as do the strategically defensive campaigns waged by the Royal Air Force and related ele-

ments in the Battle of Britain, and by hard-pressed U.S. Navy forces up through the Battle of Midway during the Pacific War.

There are always many explanations why a smaller, weaker force wins. But a crucial constant may be superior intelligence and communications, be that because of fast scouts on horseback (the Mongol "Arrow Riders"), breakthroughs in radar and cryptography (the British and American cases), or other technological and organizational innovations.

Indeed, an historical study could help illuminate not only the importance of the information factor, but also the extent to which it depends on correctly combining the technological and organizational dimensions of innovation. Such a study, along with the gaming experiment proposed above, might offer lessons for whether and how the United States could move to develop military and other forces that will be lighter and leaner yet more effective than those of any potential rival in the information age.




The next phase in our research agenda will emphasize three strands. First, the theory behind netwar must receive additional attention. In particular, the issues of offense dominance, weakened deterrence, and proactive defensive measures require analysis. At the level of applications, research will likely focus on improving interagency effectiveness. Finally, a third aspect of our research program calls for a series of in-depth case studies to test key hypotheses (e.g., the need for networks to fight networks) and to generate new insights about information-age dilemmas.

Further research will also enable us to deal in more detail with concepts that bear upon operational concerns. For example, we have hypothesized earlier in this briefing that, if networked and hierarchical forms are mixed in a netwar actor, an optimal course is to attack the hierarchical structures first. Such a targeting strategy presumes that the destruction or disruption of hierarchical elements will have resonant effects, particularly if the opponent network is of the "star" or "chain" variety. Another issue is the need to develop a methodology for assessing which targets possess the most valuable "information packages"—and whether it is indeed better to attack them than other targets.

An applied policy recommendation that may be advanced in this next phase is the creation of an "information war room," a facility that would support defensive netwar strategies, inform operational planners, and raise the probability of success by optimizing joint interagency and inter-organizational efforts. Those assigned to this facility would provide net assessments of the informational capabilities of likely netwar adversaries. They would also "map" the key nodes of opponents, identify the "high information" targets, and develop detailed "information orders of battle." It is crucial to note that both the war room and its outputs, from orders of battle to maps of an adversary's key nodes, should not be limited to, or even primarily focused

upon, cyberspace factors and components. An information order of battle will also have to consider the adversary's public media and private diplomatic resources and capabilities.

When an opponent is a state, mapping key nodes includes, but should not be limited to, its power grid, financial market structures, and other forms of electronic interconnectivity. The notion of key nodes should include some sense of an opponent's societal structures and its strong and weak points, because some, perhaps many, adversaries will have little by way of information infrastructure to hold at risk. Thus, a broader view of the mapping function may enable proportionate, if asymmetric, damage to be done if retaliation is needed against low-tech opponents who can nevertheless attack the inviting, rich targets of the U.S. "infosphere." Of course, when an opponent is a nonstate actor, different approaches to mapping and other assessments will have to be designed than is the case with states.

These are the sorts of broad issues that could be raised in an information war room, leading to the creation of lucid, usable information orders of battle. If this approach can be initiated and sustained, then the prospects for waging defensive netwar successfully will grow considerably.

Finally, in the area of comparative analyses, attention should be given to cases that combine social, political, and military factors. Mexico and Haiti come to mind as recent cases. Yet, we feel that historical analysis should not be entirely retrospective. For example, there may be significant analytic benefits to be derived from designing a hypothetical information-age netwar, one with links to a military cyberwar. The goal is an heuristic exercise that can inform and influence policy and strategy.

A classic example of this type of study can be found in the work of Hector Bywater, who wrote his visionary *The Great Pacific War* in the 1920s. Bywater speculated about a U.S.–Japan conflict and anticipated carrier-based, island-hopping amphibious warfare and even developed insights into such innovations as kamikaze attacks. At the policy level, his views had a profound effect on War Plan Orange, which, until that time, had planned to have the U.S. battle fleet traverse the breadth of the Pacific to engage the Imperial Japanese Navy in one climactic battle for naval supremacy. Perhaps a similar intellectual exercise, along the lines of a "Great Netwar," would generate equally insightful results. We hope to achieve this in a prospective book, *Society and Security in the Information Age.*

## BIBLIOGRAPHY


Allard, C. Kenneth, "The Future of Command and Control: Toward a Paradigm of Information Warfare," L. Benjamin Ederington and Michael J. Mazarr (eds.), *Turning Point: The Gulf War and U.S. Military Strategy,* Boulder: Westview Press, 1995, pp. 161–192.

———, *Somalia Operations,* Washington, D.C.: National Defense University Press, 1995.

Andelman, David A., "The Drug Money Maze," *Foreign Affairs,* July/August 1994, pp. 94–108.

Anderson, Malcolm, *Policing the World,* Oxford: Clarendon Press, 1989.

Arquilla, John, "The Strategic Implications of Information Dominance," *Strategic Review,* Summer 1994, pp. 24–30.

———, *From Troy to Entebbe: Special Operations in Ancient and Modern Times,* Lanham, Md.: University Press of America, 1996.

Arquilla, John, and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy,* Vol. 12, No. 2, pp. 141–165 (Summer 1993).

———, "(Book Review) Welcome to the Revolution . . . in Military Affairs," *Comparative Strategy,* Vol. 14, No. 2, pp. 331–341 (Spring 1995).

———, "Information, Power, and Grand Strategy: In Athena's Camp," Stuart Schwartzstein (ed.), *Information and National Security,* Washington, D.C.: Center for International and Strategic Studies, 1996.

Beam, Louis, "Leaderless Resistance," *The Seditionist,* Issue 12, February 1992 (text can sometimes be located on the Internet).

Beniger, James R., *The Control Revolution: Technological and Economic Origins of the Information Society,* Cambridge, Mass.: Harvard University Press, 1986.

Boorman, Scott, *The Protracted Game: A Weich'i Interpretation of Maoist Revolutionary Strategy,* New York: Oxford University Press, 1969.

Boulding, Elise, *Building a Global Civic Culture: Education for an Interdependent World,* New York: Teachers College Press, 1988.

Brassey's, *War Annuals, 1991–1994,* London: Brassey's, Ltd., 1991–1995.

Braudel, Fernand, *Civilization and Capitalism, 15th–18th Century, Volume II: The Wheels of Commerce,* translated from original French edition (1979), New York: Harper & Row, 1982.

Brecher, Jeremy, John Brown Childs, and Jill Cutler (eds.), *Global Visions: Beyond the New World Order,* Boston: South End Press, 1993.

Bresler, Fenton, *The Chinese Mafia,* New York: Stein and Day, 1981.

Burghardt, Tom, "Leaderless Resistance and the Oklahoma City Bombing," San Francisco, Calif.: Bay Area Coalition for Our Reproductive Rights (BACORR), April 1995a.

———, "Dialectics of Terror: A National Directory of the Direct Action Anti-Abortion Movement and Their Allies," San Francisco, Calif.: Bay Area Coalition for Our Reproductive Rights (BACORR), October 1995b.

Bywater, Hector C., *The Great Pacific War,* New York: St. Martin's Press, 1924; reprinted 1991.

Castañeda, Jorge G., *The Mexican Shock: Its Meaning for the United States,* New York: The New Press, 1995.

Chairman of the Joint Chiefs of Staff, *Memorandum of Policy Number 30,* Washington, D.C., 1993.

Chase, Alston, *In a Dark Wood: The Fight over Forests and the Rising Tyranny of Ecology,* New York: A Richard Todd Book/Houghton Mifflin Company, 1995.

Chisholm, Donald, *Coordination Without Hierarchy: Informal Structures in Multi-organizational Systems,* Berkeley: University of California Press, 1989.

Claessen, Henri J.M., and Peter Skalník (eds.), *The Early State,* The Hague: Mouton Publishers, 1978.

Cleaver, Harry, "Introduction," Editorial Collective, *¡Zapatistas! Documents of the New Mexican Revolution,* Brooklyn: Autonomedia, 1994 (on-line at gopher://lanic.utexas.edu:70/11/la/Mexico/ Zapatistas/).

Clutterbuck, Richard, *Terrorism, Drugs, and Crime in Europe after 1992,* New York: Routledge, 1990.

Cobban, Helena, *The Palestinian Liberation Organization,* Cambridge: Cambridge University Press, 1984.

Cohen, Frederick B., *Protection and Security on the Information Superhighway,* New York: John Wiley and Sons, 1995.

Cohen, Ronald, and Elman R. Service (eds.), *Origins of the State: The Anthropology of Political Evolution,* Philadelphia: Institute for the Study of Human Issues (ISHI), 1978.

Collins, Larry, and Dominique Lapierre, *The Fifth Horseman,* New York: Simon & Schuster, 1979.

Davis, Paul K., and John Arquilla, *Deterring or Coercing Opponents in Crisis: Lessons from the War with Saddam Hussein,* Santa Monica, Calif.: RAND, R-4111-JS, 1991a.

———, *Thinking About Opponent Behavior in Crisis and Conflict: A Generic Model for Analysis and Group Discussion,* Santa Monica, Calif.: RAND, N-3322-JS, 1991b.

Delbrück, Hans, *History of the Art of War,* 4 vols., Lincoln: University of Nebraska Press, 1900; revised 1990.

Drucker, Peter F., *Post-Capitalist Society,* New York: HarperCollins Publishers, 1993.

———, "The Age of Social Transformation," *Atlantic Monthly,* November 1994, pp. 53–80.

Evans-Pritchard, E. E., *The Nuer: A Description of the Modes of Livelihood and Political Institutions of a Nilotic People,* Oxford: Oxford University Press, 1940.

Fischer, David Hackett, *Paul Revere's Ride,* New York: Oxford University Press, 1994.

Frederick, Howard, "Computer Networks and the Emergence of Global Civil Society," Linda M. Harasim (ed.), *Global Networks: Computers and International Communication,* Cambridge, Mass.: The MIT Press, 1993, pp. 283–295.

Fried, Morton H., *The Evolution of Political Society: An Essay in Political Anthropology,* New York: Random House, 1967.

Galvin, John R., *The Minute Men: The First Fight: Myths & Realities of the American Revolution,* Washington, D.C.: Pergamon-Brassey's International Defense Publisher, 2nd ed., revised, 1989.

Gann, Lewis, *Guerrillas in History,* Stanford: Hoover Institution Press, 1971.

Gelernter, David, *Mirror Worlds, or the Day Software Puts the Universe in a Shoebox . . . How It Will Happen and What It Will Mean,* New York: Oxford University Press, 1991.

Gerlach, Luther P., "Protest Movements and the Construction of Risk," B. B. Johnson and V. T. Covello (eds.), *The Social and Cultural Construction of Risk,* Boston: D. Reidel Pub. Co., 1987, pp. 103–145.

Gerlach, Luther P., and Virginia Hine, *People, Power, Change: Movements of Social Transformation,* New York: The Bobbs-Merrill Co., Inc., 1970.

Gibson, Clark Campion, *Politicians, Peasants and Poachers: The Political Economy of Wildlife Policy in Zambia, 1964–1991,* Ph.D. dissertation, Duke University, 1995.

Gipson, Lawrence H., *The Great War for Empire: The Years of Defeat,* New York: Alfred A . Knopf, 1946.

Gonzalez, Edward, and David Ronfeldt, *Storm Warnings for Cuba*, Santa Monica, Calif.: RAND, MR-452-0SD, 1994.

Goren, Roberta, *The Soviet Union and Terrorism*, London: Allen & Unwin, 1984.

Granovetter, Mark S., "Economic Action and Social Structure: The Problem of Embeddedness," *American Journal of Sociology*, Vol. 91, No. 3, November 1985, pp. 481–510.

Graves, Robert, *The Greek Myths*, Penguin Books, Baltimore, Md., 1960.

Hafner, Katie, and John Markoff, *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, New York: Simon and Schuster, 1991.

Hamilton, Edith, *Mythology*, Little, Brown, and Co., Boston, Mass., 1969.

Handel, Michael, *Sun Tzu and Clausewitz Compared*, Carlisle, Pa.: Strategic Studies Institute, 1991.

Hannerz, Ulf, *Cultural Complexity: Studies in the Social Organization of Meaning*, New York: Columbia University Press, 1992.

Heclo, Hugh, "Issue Networks and the Executive Establishment," Anthony King (ed.), *The New American Political System*, Washington, D.C.: The American Enterprise Institute, 1978, pp. 87–124.

Heilbroner, Robert L., *The Worldly Philosophers: The Lives, Times, and Ideas of the Great Economic Thinkers*, New York: Simon & Schuster, 3rd ed., revised, 1967.

Hirschman, Albert O., *The Passions and the Interests: Political Arguments for Capitalism Before Its Triumph*, Princeton: Princeton University Press, 1977.

Hoffman, Bruce, *Responding to Terrorism Across the Technological Spectrum*, Santa Monica, Calif.: RAND, P-7874, 1994.

Hundley, Richard O., and Robert H. Anderson, *Security in Cyberspace: An Emerging Challenge for Society*, Santa Monica, Calif.: RAND, P-7893, 1994.

Ianni, Francis A. J., *Black Mafia: Ethnic Succession in Organized Crime*, New York: Simon & Schuster, 1974.

Jacobs, Jane, *Systems of Survival: A Dialogue on the Moral Foundations of Commerce and Politics*, New York: Random House, 1992.

Johnson, Allen W., and Timothy Earle, *The Evolution of Human Societies: From Foraging Group to Agrarian State*, Stanford: Stanford University Press, 1987.

Kahn, Herman, *On Thermonuclear War*, Princeton: Princeton University Press, 1960.

Kaplan, David, and Alex Dubro, *Yakuza*, Reading, Mass.: Addison-Wesley, 1986.

Kedzie, Chris, "Democracy and Network Interconnectivity" (Proceedings of INET '95, Honolulu, June 1995).

Kelly, Kevin, *Out of Control: The Rise of Neo-Biological Civilization,* New York: Addison-Wesley Publishing Company, 1994.

Kissinger, Henry, *Nuclear Weapons and Foreign Policy,* New York: Council on Foreign Relations Press, 1957.

Krepinevich, Andrew F., Jr., *The Army and Vietnam,* Baltimore, Md.: Johns Hopkins University Press, 1986.

Kumon, Shumpei, "Japan as a Network Society," Shumpei Kumon and Henry Rosovsky (eds.), *The Political Economy of Japan, Volume 3: Cultural and Social Dynamics,* Stanford: Stanford University Press, 1992, pp. 109–141.

Kupperman, Robert and Jeff Kamen, *Final Warning: Averting Disaster in the New Age of Terrorism,* New York: Doubleday, 1989.

Laquer, Walter, *Terrorism,* Boston: Little, Brown, 1979.

Laraña, Enrique, Hank Johnston, and Joseph R. Gusfield, eds., *New Social Movements: From Ideology to Identity,* Philadelphia, Pa.: Temple University Press, 1994.

Libicki, Martin C., *The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon,* Washington, D.C.: National Defense University Press, 1994.

Liddell Hart, B.H., *Strategy,* London: Faber & Faber, Ltd., 1954.

Lindblom, Charles E., *Politics and Markets: The World's Political-Economic Systems,* New York: Basic Books, Inc., 1977.

Lipnack, Jessica, and Jeffrey Stamps, *The Age of the Network,* Essex Junction, Vt.: Oliver Wight Publications, Inc., 1994.

Littleton, Matthew, *Information Age Terrorism,* M.A. thesis, Monterey, Calif.: Naval Postgraduate School, 1995.

Maslow, Abraham, *Motivation and Personality,* 3rd ed. [with new material by Ruth Cox and Robert Frager], New York: Harper and Row, 1987.

Mill, J. S., "A Few Words on Non-Intervention," *Essays on Politics,* New York: Doubleday, 1857; reprinted 1962, pp. 396–413.

Morris, Aldon D., and Carol McClurg (eds.), *Frontiers in Social Movement Theory,* New Haven: Yale University Press, 1992.

Nohria, Nitin, and Robert G. Eccles (eds.), *Networks and Organizations: Structure, Form, and Action,* Boston, Mass.: Harvard Business School Press, 1992.

North, Douglass C., *Structure and Change in Economic History,* New York: W. W. Norton & Co., 1981.

Ohmae, Kenichi, *The End of the Nation-State: The Rise of Regional Economies,* New York: The Free Press, 1995.

Parkman, Francis, *Montcalm and Wolfe: The Decline and Fall of the French Empire in North America,* New York: Collier, 1884; reprinted 1962.

Perrow, Charles, *Complex Organizations: A Critical Essay,* 2nd Edition, Glenview, Ill.: Scott, Foresman and Company, 1979.

Poggi, Gianfranco, *The Development of the Modern State: A Sociological Introduction,* Stanford: Stanford University Press, 1978.

Polanyi, Karl, *The Great Transformation,* Boston, Mass.: Beacon Press, 1944; reprinted 1957.

Powell, Walter W., "Neither Market Nor Hierarchy: Network Forms of Organization," Barry M. Staw and L. L. Cummings, ed., *Research in Organizational Behavior: An Annual Series of Analytical Essays and Critical Reviews,* Vol. 12, Greenwich, Conn.: JAI Press Inc., 1990, pp. 295–336.

Powell, Walter W., and Laurel Smith-Doerr, "Networks and Economic Life," Neil J. Smelser and Richard Swedberg, eds., *The Handbook of Economic Sociology,* Princeton, N.J.: Princeton University Press & Russell Sage Foundation, 1994, pp. 368–402 (Chapter 15).

Quester, George, *Offense and Defense in the International System,* New York: John Wiley, 1977.

Reich, Walter, ed., *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind,* Cambridge, Mass.: Cambridge University Press, 1990.

Reisman, W. Michael, and James E. Baker, *Regulating Covert Action,* New Haven, Conn.: Yale University Press, 1992.

Rivers, Gayle, *The War Against the Terrorists: How to Win It,* New York: Stein and Day, 1986.

Ronfeldt, David, "Cyberocracy Is Coming," *The Information Society,* Vol. 8, No. 4, 1992, pp. 243–296.

———, *Institutions, Markets, and Networks: A Framework About the Evolution of Societies,* Santa Monica, Calif.: RAND, DRU-590-FF, December 1993.

———, *Tribes, Institutions, Markets, Networks—A Framework About Societal Evolution,* Santa Monica, Calif.: RAND, P-7967, 1996.

Ronfeldt, David, and Cathryn Thorup, *North America in the Era of Citizen Networks: State, Society, and Security,* Santa Monica, Calif.: RAND, P-7945, 1995.

Rothschild, Emma, "What Is Security?" *Daedalus,* Vol. 124, No. 3, Summer 1995, pp. 53–98.

Sahlins, Marshall D., *Tribesmen,* Englewood Cliffs: Prentice-Hall, 1968.

Salamon, Lester M., "The Rise of the Nonprofit Sector," *Foreign Affairs,* Vol. 73, No. 4, July/August 1994, pp. 109–122.

Schelling, Thomas C., *Arms and Influence,* New Haven, Conn.: Yale University Press, 1966.

Schwartau, Winn, *Information Warfare: Chaos on the Electronic Superhighway,* New York: Thunder's Mouth Press, 1994.

Service, Elman R., *Primitive Social Organization, An Evolutionary Perspective,* Second Edition, New York: Random House, 1971.

———, *Origins of the State and Civilization: The Process of Cultural Evolution,* New York: W.W. Norton and Company, 1975.

Shils, Edward, "The Virtue of Civil Society," *Government and Opposition,* Vol. 26, No. 1, Winter 1991, pp. 3–20.

Skolnikoff, Eugene B., *The Elusive Transformation: Science, Technology, and the Evolution of International Politics,* Princeton, N.J.: Princeton University Press, 1993.

Smith, Arthur, *The Game of Go,* New York: Moffat, Yard and Co., 1908.

Spiro, Peter J., "New Global Communities: Nongovernmental Organizations in International Decision-Making Institutions," *The Washington Quarterly,* Vol. 18, No. 1, Winter 1995, pp. 45–56.

Sterling, Claire, *Thieves' World: The Threat of the New Global Network of Organized Crime,* New York: Simon & Schuster, 1994.

Stern, Kenneth, *A Force upon the Plain: The American Militia Movement and the Politics of Hate,* New York: Simon & Schuster, 1996.

Stockholm International Peace Research Institute, *World Annuals, 1991–1994.*

Strassmann, Paul A., *The Politics of Information Management,* New Canaan, Conn.: The Information Economics Press, 1995.

Summers, Harry G., Jr., *On Strategy: A Critical Analysis of the Vietnam War,* Novato, Calif.: Presidio Press, 1982.

Szafranski, Colonel Richard, "Neo-Cortical Warfare? The Acme of Skill," *Military Review,* November 1994, pp. 41–55.

———, "A Theory of Information Warfare: Preparing for 2020," *Airpower Journal,* Spring 1995, pp. 56–65.

Tainter, Joseph A., *The Collapse of Complex Societies,* New York: Cambridge University Press, 1988.

Thorup, Cathryn L. "Politics of Free Trade and the Dynamics of Cross-Border Coalitions in U.S.-Mexican Relations," *Columbia Journal of World Business,* Vol. XXVI, No. II, Summer 1991, pp. 12–26.

———, *Redefining Governance in North America: The Impact of Cross-Border Networks and Coalitions on Mexican Immigration into the United States*, Santa Monica, Calif.: RAND, DRU-219-FF, 1993.

———, "Building Community Through Participation: The Role of Non-Governmental Actors in the Summit of the Americas," Robin Rosenberg and Steven Stein, eds., *Advancing the Miami Process: Civil Society and the Summit of the Americas*, Coral Gables, Fl.: North-South Center Press, 1995, pp. xiii–xxvi.

Toffler, Alvin, *Future Shock*, New York: Random House Inc., 1970.

———, *Powershift: Knowledge, Wealth, and Violence at the Edge of the 21st Century*, New York: Bantam Books, 1990.

Toffler, Alvin, and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the Twenty-first Century*, Boston, Mass.: Little, Brown and Company, 1993.

Van Creveld, Martin, *Technology and War: From 2000 B.C. to the Present*, New York: The Free Press, 1989.

———, *The Transformation of War*, New York: Free Press, 1991.

Vaksberg, Arkady, *The Soviet Mafia*, New York: St. Martin's Press, 1992.

*Violence at Sea Database*, Monterey, Calif.: Naval Postgraduate School, 1995.

Walzer, Michael, "The Idea of Civil Society: A Path to Social Reconstruction," *Dissent*, Spring 1991, pp. 293–304.

Wapner, Paul, "Politics Beyond the State: Environmental Activism and World Civic Politics," *World Politics*, Vol. 47, No. 3, April 1995, pp. 311–340.

Weinberger, Caspar, "The Uses of Military Force," Speech to the National Press Club, November 28, 1984.

Williams, Phil, "Transnational Criminal Organizations and International Security," *Survival*, Vol. 36, No. 1, Spring 1994, pp. 96–113.

———, "Transnational Criminal Organizations: Strategic Alliances," *The Washington Quarterly*, Vol. 18, No. 1, Winter 1995, pp. 57–72.

Williamson, Oliver E., *Markets and Hierarchies: Analysis and Antitrust Implications*, New York: The Free Press, 1975.

Wylie, J. C., *Military Strategy: A General Theory of Power Control*, New Brunswick, N.J.: Rutgers University Press, 1967.